Taming the Hacker Storm

A Framework for Defeating Cybercriminals and Malware

Roger A. Grimes
Data-Driven Defense Evangelist,
KnowBe4, Inc.
rogerg@knowbe4.com

Roger A. Grimes
Data-Driven Defense Evangelist
KnowBe4, Inc.

email: rogerg@knowbe4.com
Twitter/X : @RogerAGrimes
LinkedIn: https://www.linkedin.com/in/rogeragrimes/
Mastodon: https://infosec.exchange/@rogeragrimes
YouTube: @CyberSecWTFRants
Bluesky: rogeragrimes@bsky.social

About Roger

- 36 years plus in computer security, 20 years pen testing
- Expertise in host and network security, IdM, crypto, PKI, APT, honeypot, cloud security
- Consultant to world's largest companies and militaries for decades
- Previous worked for Foundstone, McAfee, Microsoft
- Written 15 books and over 1,500 magazine articles
- *InfoWorld* and *CSO* weekly security columnist 2005 - 2019
- Frequently interviewed by magazines (e.g., Newsweek) and radio shows (e.g., NPR's All Things Considered)

Certification exams passed include:

- CPA
- CISSP, CISM, CISA
- MCSE: Security, MCP, MVP
- CEH, TISCA, Security+, CHFI, yada, yada

Roger’s Books

ROGER A. GRIMES
HACKING MULTIFACTOR AUTHENTICATION
ROGER A. GRIMES
A DATA-DRIVEN COMPUTER DEFENSE
A WAY TO IMPROVE ANY COMPUTER DEFENSE
THIRD EDITION
(ISC)²
HACKING THE HACKER
RTS WHO TAKE DOWN HACKERS
R A. GRIMES
WILEY
Internet Computer Security
Malicious Mobile Code
Virus Protection for Windows
O'REILLY
The Complete Reference
Network Security
MORE THAN 20 CO-AUTHORS AND TECHNICAL REVIEWERS
RANSOMWARE PROTECTION PLAYBOOK
ROGER A. GRIMES
WILEY
Cryptography Apocalypse
paring for the Day When Quantu nputing Breaks Today's Crypto
Roger A. Grim
WILEY
FIGHTING PHISHING
EVERYTHING YOU CAN DO TO FIGHT SOCIAL ENGINEERING AND PHISHING
ROGER A. GRIMES WITH DR. JOHN N. JUST
WILEY
ROGER A. GRIMES
TAMING THE HACKING STORM
A FRAMEWORK FOR DEFEATING HACKERS AND MALWARE
Windows Desktop and Server Hardening
wrox
Windows Server 2008 Security Resource Kit
Microsoft
WINDOWS VISTA SECURITY
Securing Vista Against Malicious Attacks
Roger A. Grimes
Jesper M. Johansson
MCSE CORE ELECTIVE EXAMS IN A NUTSHELL
A Desktop Quick Reference
O'REILLY
Pawan K. Bhardwaj & Roger A. Grimes
THE EXPERT'S VOICE
Honeypots for Windows
Roger A. Grimes
Apress

About ▶ KnowBe4

We help over 70,000 organizations build a strong security culture to manage the ongoing problem of social engineering and human risk.

G2

Top 100

Global Software Companies

BEST SOFTWARE AWARDS

2024

Trusted by 47 of the world's top 50 cybersecurity companies, and the largest human risk management platform

Gartner®

Magic Quadrant Leader

Global Sales, Courseware Development, Customer Success, and Technical Support teams worldwide

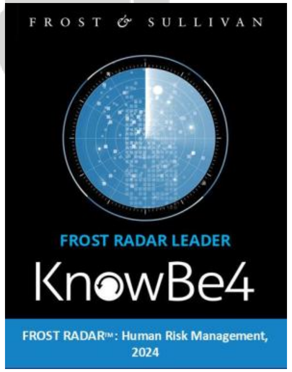
TrustRadius

Top Rated

2024

★ ★ ★ ★ ★

CEO, leadership and Knowsters are industry veterans in cybersecurity



FROST & SULLIVAN

FROST RADAR LEADER

KnowBe4

FROST RADAR™: Human Risk Management, 2024

Office in the USA, UK, Canada, France, Netherlands, India, Germany, South Africa, United Arab Emirates, Singapore, Japan, Australia, and Brazil

So far, every single cyber defense that has been created has utterly failed to significantly mitigate hackers and malware

Agenda

KnowBe4

- How Bad Is It?
- The Main Underlying Problem
- The Solution
- Other Needed Solutions

Agenda

KnowBe4

- How Bad Is It?
- The Main Underlying Problem
- The Solution
- Other Needed Solutions

How Bad Is It?

The Internet - Statistics

- There are over 1.12 billion websites worldwide, over 250K new ones are added each day, and
  - **10% of new websites are malicious**
- Google’s Safe Browsing service detects over 3M potentially malicious URLs every day

Most malicious websites are very temporary

- **Microsoft states that 70% of malicious sites are active for less than two hours**

- **Per Google, the average malicious website exists for less than 10 minutes**

How Bad Is It?

<u>The Malicious Internet - Statistics</u>

Most traffic on the Internet is malicious

- **Arkose Labs said 73% of Internet traffic is malicious**

<u>Bad Bots Alone Are 33% of the Problem</u>

- Forbes stated that bad bot traffic is at least a third of all Internet traffic

- Cloudflare’s 2024 State of Application Security states that **nearly one-third of all Internet traffic stems from bots, 93% of which appear malicious**

How Bad Is It?

The Malicious Internet - Statistics

Most email is malicious

- **57% of all sent emails are malicious**
- Gmail blocks 100 million malicious emails per day
- Microsoft blocks 31.5B emails/year or 1100/second
- **1 in 7 bad emails makes it past defenses**

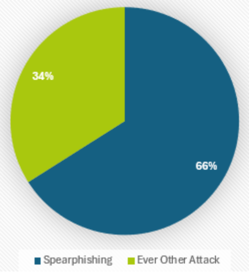
How Bad Is It?

The Malicious Internet - Statistics

Phishing is the Biggest Cause of Successful Hacking

- 70% - 90% of all Internet crime involves social engineering

- Barracuda Networks reported that while spear-phishing emails make up less than 0.1% of all email attacks, they are responsible for 66% of all successful breaches. One thing…responsible for two-thirds of all attacks



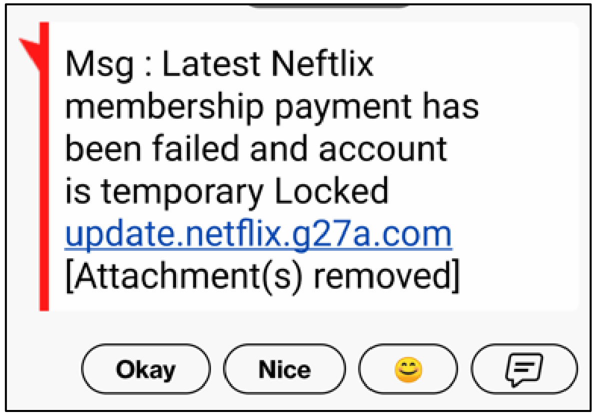
How Bad Is It?

The Malicious Internet - Statistics

A lot of texting is malicious

- More than 1 billion unwanted SMS/min and at least 1M of those are intentionally malicious

- TechJury states that 8.9% - 14.5% of recipients click on malicious links in text messages



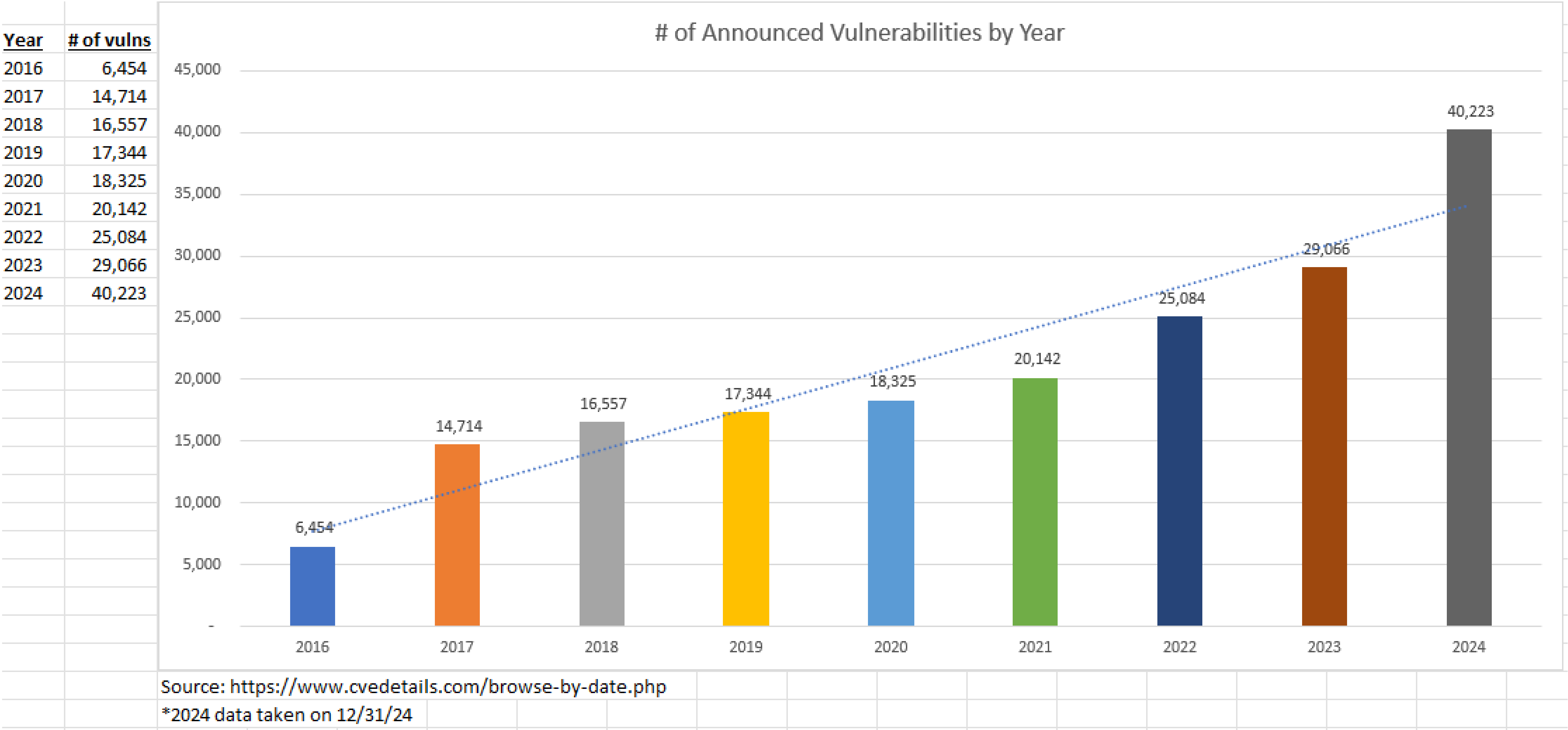
Msg : Latest Neftlix membership payment has been failed and account is temporary Locked update.netflix.g27a.com [Attachment(s) removed]

How Bad Is It?

Vulnerabilities- Statistics

- Google's Mandiant, stated that 33% of data breaches involve software and firmware vulnerabilities

How Bad Is It?



Year	# of vulns
2016	6,454
2017	14,714
2018	16,557
2019	17,344
2020	18,325
2021	20,142
2022	25,084
2023	29,066
2024	40,223

# of Announced Vulnerabilities by Year

Source: https://www.cvedetails.com/browse-by-date.php

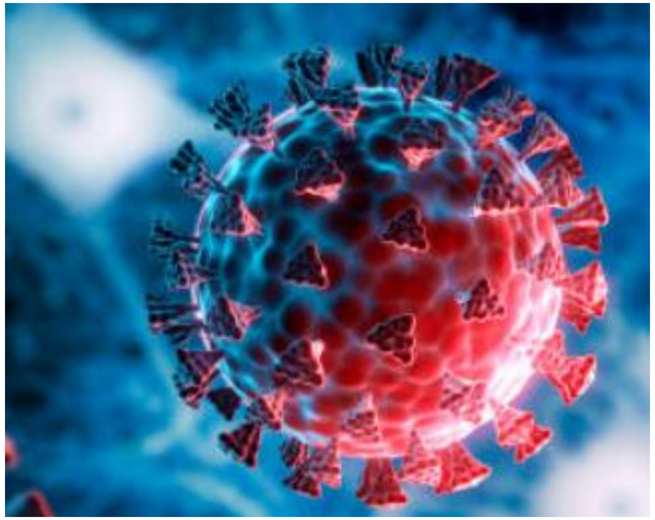
*2024 data taken on 12/31/24

What isn't as widely known is that only 1% of all publicly announced vulnerabilities are ever used by a real-world attacker against a real-world target.

How Bad Is It?

Malware

- There are over individual 1B malware programs
- 450K-560K new malware programs are detected every day



How Bad Is It?

How Common Are Breaches- Statistics

Over 40% of organizations experience a data breach each year, according to these reports:

- GetApp's 2024 Data Security Report states that 44% of U.S. organizations and 51% of global organizations experienced a ransomware attack in the last 12 months
- Ponemon stated 52% of respondents have experienced a data breach…in the last 12 months
- 40% of Fortune 1000 companies will suffer a breach every year
- Cymulate stated that 40% of respondents admitted to being breached over the past 12 months. After being breached once, 66% of breached respondents said they suffered additional attacks

Agenda

KnowBe4

- How Bad Is It?
- The Main Underlying Problem
- The Solution
- Other Needed Solutions

The Main Problem

Main Question

- **Why do we have so many hackers and malware programs for so long?**

- The Internet gives nearly infinite scale, easily exploitable, access to potential victims (people and devices)

Better Answer

- We cannot stop, identify, block, or arrest hackers!!
- Largely, because we don’t know who they are and they can claim to be whoever they want in each attack

The Main Problem

Main Questio

- **Why do we h and malware programs fo**

- The Internet e, easily exploitable, access to pote l devices)

Better Answer

- We cannot sto est hackers!!
- Largely, becau hey are and they can claim to b each attack

The Main Problem

Main Problem

- Rob a bank in person, likely get caught, identified, arrested, charged, tried, and put in jail

There were 1263 bank robberies in 2023, with an average take of $4200

- Rob a bank, company, or person online and rarely get held accountable
- All profit, very little risk

The Main Problem

Main Problem

- We cannot reliably identify hackers and their creations
  - We do not know who they really are, and because of that:
    - We cannot stop them
    - We cannot reliably block them
    - We cannot punish them
    - We cannot arrest them

- Cybercrime is often done from other countries (no way to arrest and enforce laws even if we could identity them)
- It’s all profit and very little risk
- It’s the perfect recipe for encouraging lawlessness

Agenda

KnowBe4

- How Bad Is It?
- The Main Underlying Problem
- The Solution
- Other Needed Solutions

The Solution – Pervasive Selective Trust

Everything we do is about trust…or lack of trust

The Solution – Pervasive Selective Trust

Trust

- Something/someone you are interacting with is who they say they are and acts as expected

- Are you who you say you are?
- Is that program, service, app, link, file, phone number, message, or content what it says it is?

The Solution – Pervasive Selective Trust

Main Solution

- Make it harder for hackers to hide their true identity
- Allow anyone to validate anyone else's true identity when they are getting ready to interact, if desired
- **"Real ID"**
- Along with other components of trust
- **Pervasive High-Trust Ecosystem**

  Replacing pervasive anonymity

The Solution – Pervasive Selective Trust

3 Types of Identities

- **Real ID** (strongly assured, tied to real human identity)
- **Pseudo-identity** (same as most Internet identities today)
- **Attempted anonymity**

- On every connection, anyone can choose what identity and type of identity to provide or require from the other side for the connection to go forward

The Solution – Identity Proofing

Assurance

- Someone has verified that you are who you say you are

Identity proofing

- Are you who you say you are?
- Usually done by a *trusted identity service provider* providing the ID
- Can be weakly to strongly assured
  - **Weak** – confirmed via email
  - **Medium** – in-between assurance, ex. corporate verification
  - **Strong** – must meet in person, bring official identity documents, background research, etc.

Personas

Summary

- We all have different IDs for different uses (e.g., work, personal, etc.)

- Many of us are employees, co-workers, friends, spouses, parents, maybe grandparents to different people…all at the same time

- An Internet trusted identity ecosystem will have to support multiple personas per person

Personas

PersonaA

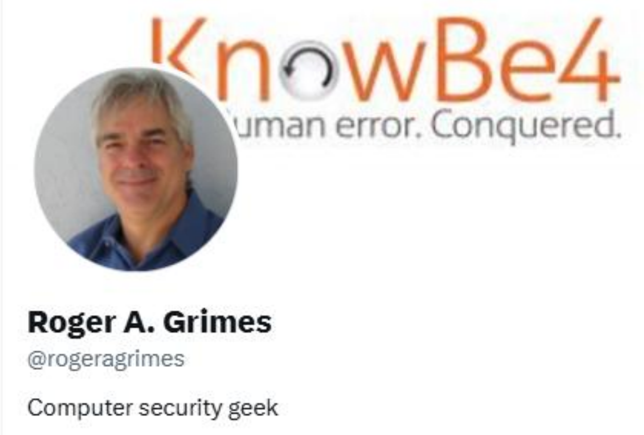
Real ID

- Roger A. Grimes
- rogerg@knowbe4.com
- Employer: KnowBe4, Inc.
- Age: 58

PersonaC

Pseudo-identity

- @rogeragrimes
- Joined March 2011



KnowBe4

uman error. Conquered.

Roger A. Grimes

@rogeragrimes

Computer security geek

PersonaB

Real ID

- Roger A. Grimes
- rogerg@banneretcs.com
- City: Tampa, FL
- Yes, older than 21

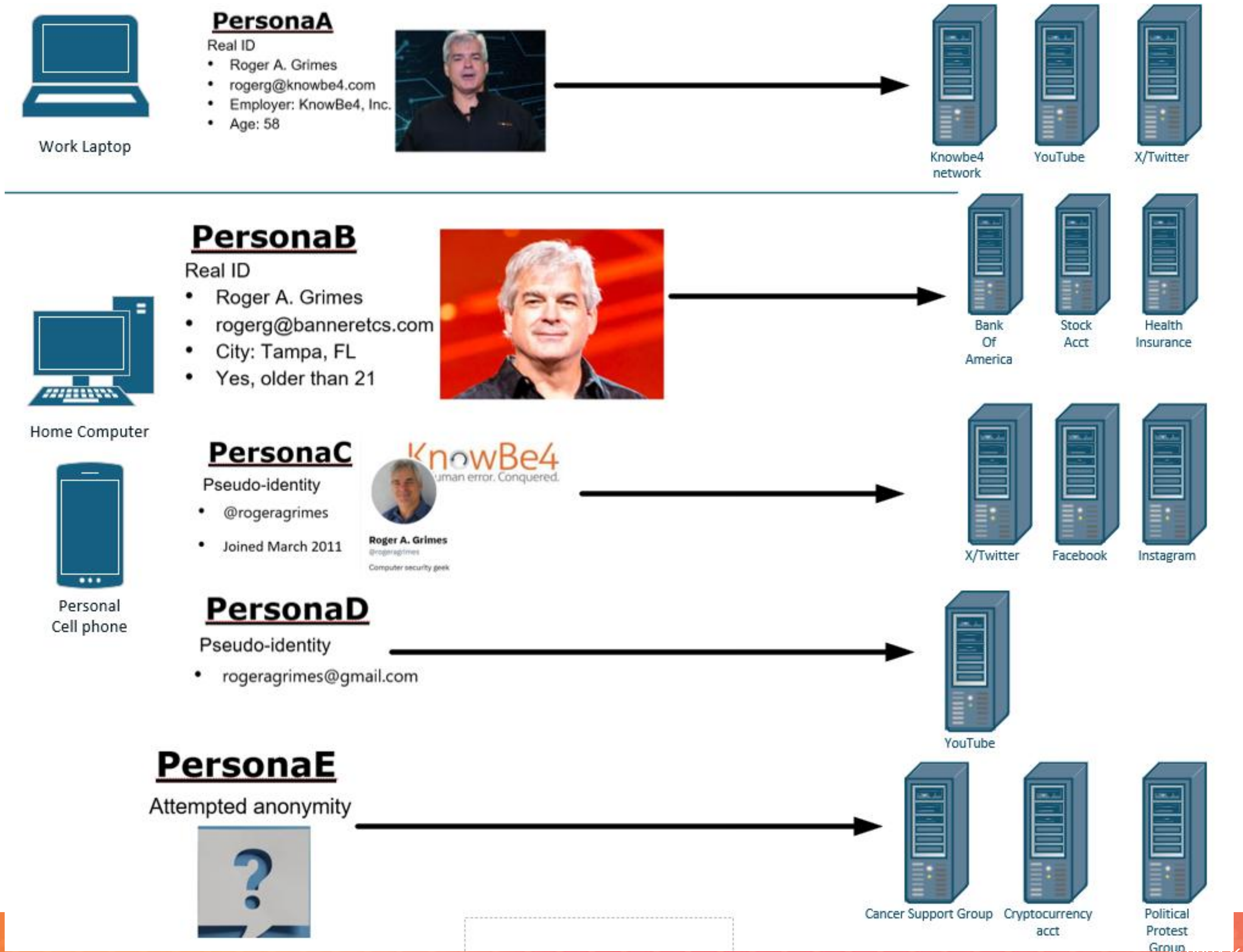
PersonaD

Pseudo-identity

- rogeragrimes@gmail.com

PersonaE

Attempted anonymity



Work Laptop

PersonaA

Real ID

- Roger A. Grimes
- rogerg@knowbe4.com
- Employer: KnowBe4, Inc.
- Age: 58

Knowbe4 network

YouTube

X/Twitter

Home Computer

PersonaB

Real ID

- Roger A. Grimes
- rogerg@banneretcs.com
- City: Tampa, FL
- Yes, older than 21

Bank Of America

Stock Acct

Health Insurance

Personal Cell phone

PersonaC

Pseudo-identity

- @rogeragrimes
- Joined March 2011

X/Twitter

Facebook

Instagram

PersonaD

Pseudo-identity

- rogeragrimes@gmail.com

YouTube

PersonaE

Attempted anonymity

Cancer Support Group

Cryptocurrency acct

Political Protest Group

But we need more than Trusted User IDs

We Need a Whole Pervasive Trusted Ecosystem

The Full Solution

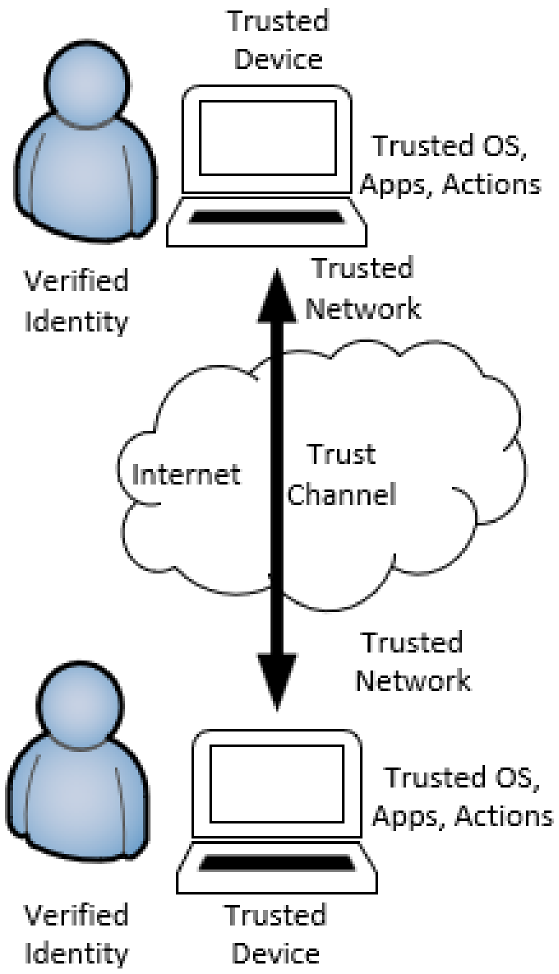
Pervasive Trusted Ecosystem

- Trusted Verified **Identities**

  plus

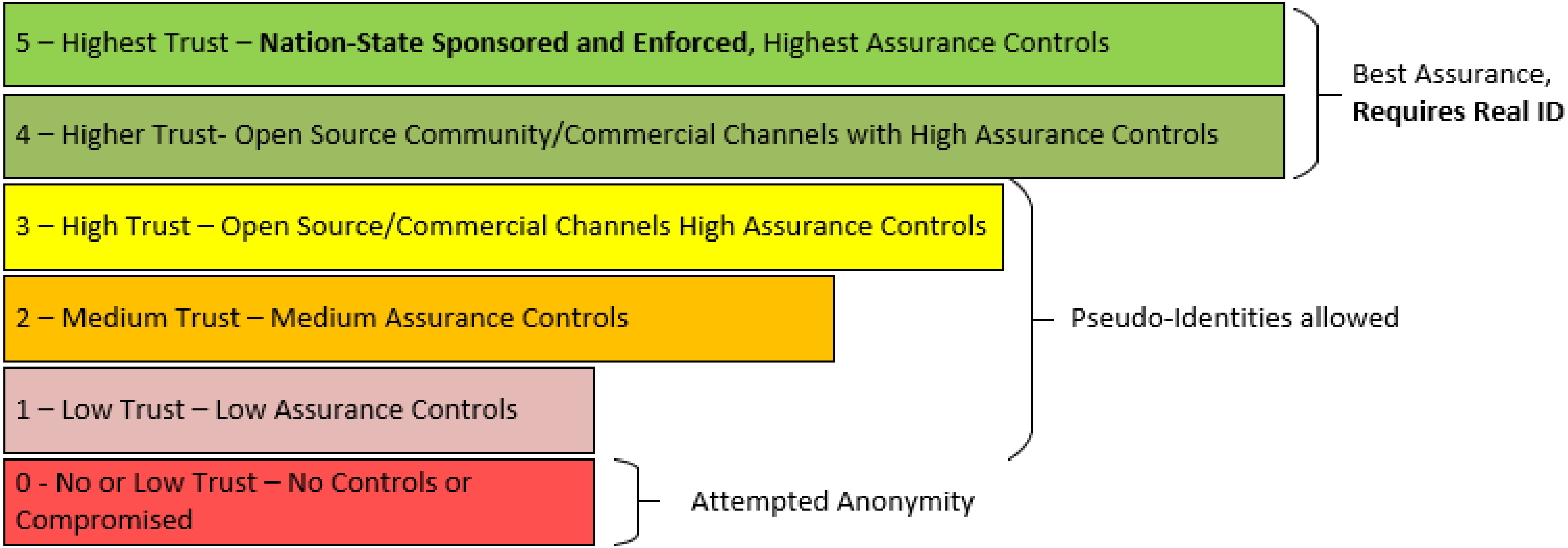
- Trusted **Devices**
- Trusted **Operating Systems**
- Trusted **Applications**
- Trusted **Actions**
- Trusted **Networks**
- **Trust Assurance Services**

= Trust Stack



The Solution

Example Trust Assurance Levels



5 – Highest Trust – **Nation-State Sponsored and Enforced,** Highest Assurance Controls

4 – Higher Trust- Open Source Community/Commercial Channels with High Assurance Controls

3 – High Trust – Open Source/Commercial Channels High Assurance Controls

2 – Medium Trust – Medium Assurance Controls

1 – Low Trust – Low Assurance Controls

0 - No or Low Trust – No Controls or Compromised

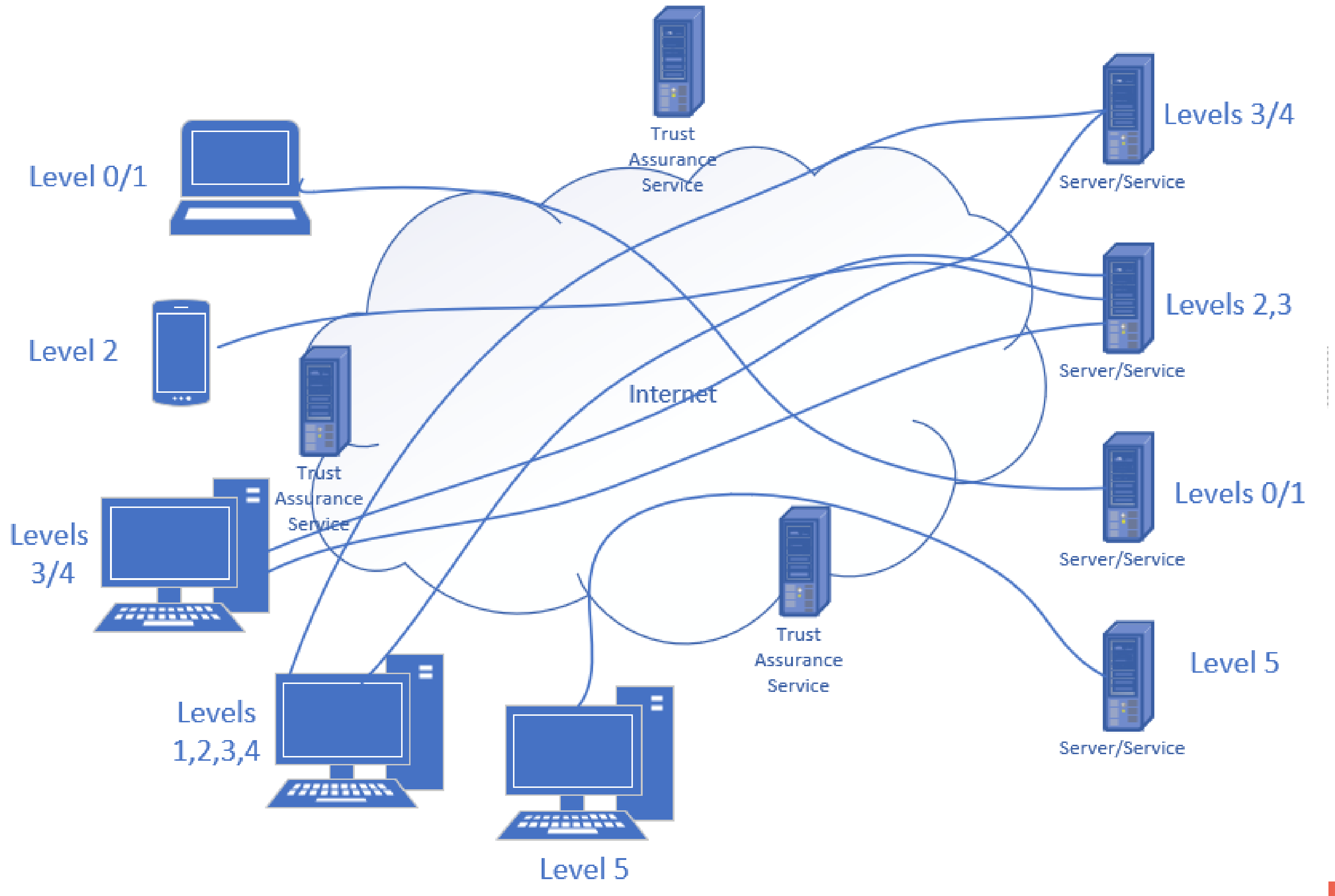
Best Assurance, **Requires Real ID**

Pseudo-Identities allowed

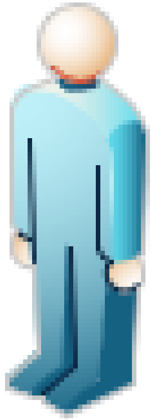
Attempted Anonymity

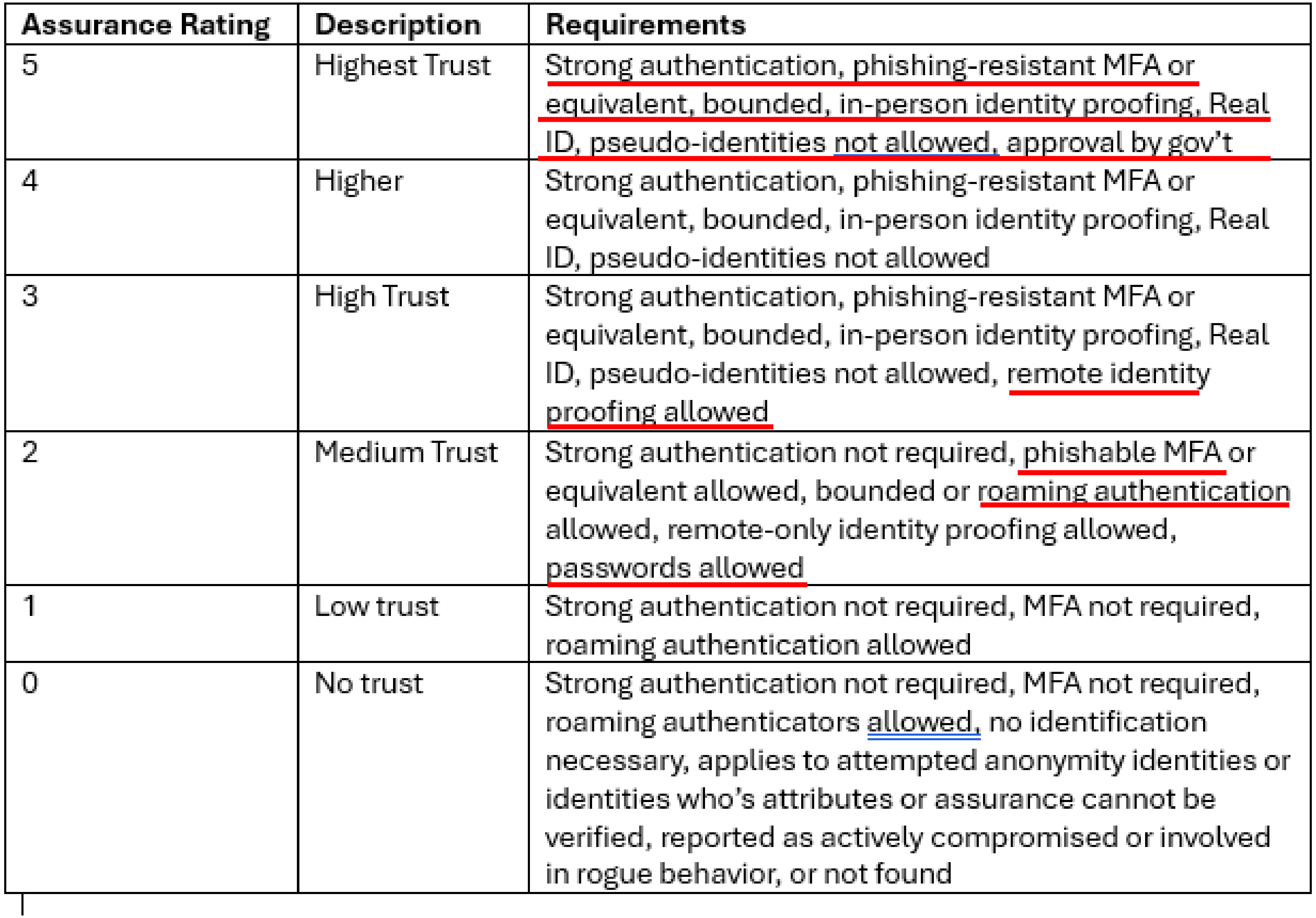
The Solution

Internet Trust Ecosystem Logical Overview



The Solution – Identity Trust Assurance Levels





Assurance Rating	Description	Requirements
5	Highest Trust	Strong authentication, phishing-resistant MFA or equivalent, bounded, in-person identity proofing, Real ID, pseudo-identities not allowed, approval by gov't
4	Higher	Strong authentication, phishing-resistant MFA or equivalent, bounded, in-person identity proofing, Real ID, pseudo-identities not allowed
3	High Trust	Strong authentication, phishing-resistant MFA or equivalent, bounded, in-person identity proofing, Real ID, pseudo-identities not allowed, remote identity proofing allowed
2	Medium Trust	Strong authentication not required, phishable MFA or equivalent allowed, bounded or roaming authentication allowed, remote-only identity proofing allowed, passwords allowed
1	Low trust	Strong authentication not required, MFA not required, roaming authentication allowed
0	No trust	Strong authentication not required, MFA not required, roaming authenticators allowed, no identification necessary, applies to attempted anonymity identities or identities who's attributes or assurance cannot be verified, reported as actively compromised or involved in rogue behavior, or not found

Requires Very Strong ID and Authentication

The Full Solution

Safe and Secure Devices

- Trusted Hardware Boot
- Verified Device Identities

The Full Solution

Trusted Hardware Boot

- Starts with a cryptographic “root of trust” chip that stores and enforces integrity
- Trusted Platform Module (TPM)
- Secure Enclave/T2 (Apple)

First version 2003

In Windows Vista
machines starting in 2007

An example Trusted Platform Module, the Infineon SLB9655TT12

In most Apple devices
since 2012

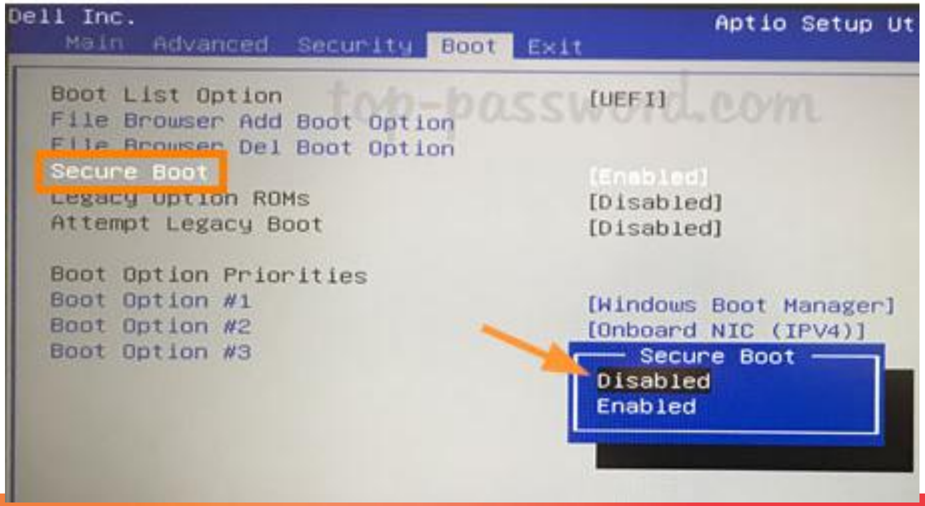
https://en.wikipedia.org/wiki/Trusted_Platform_Module

https://support.apple.com/guide/security/secure-enclave-sec59b0b31ff/web

The Full Solution

Trusted Hardware Boot

- Hardware Boot
- Hardware Secure Boot
- BIOS/UEFI protected
- Secure hand off to the OS

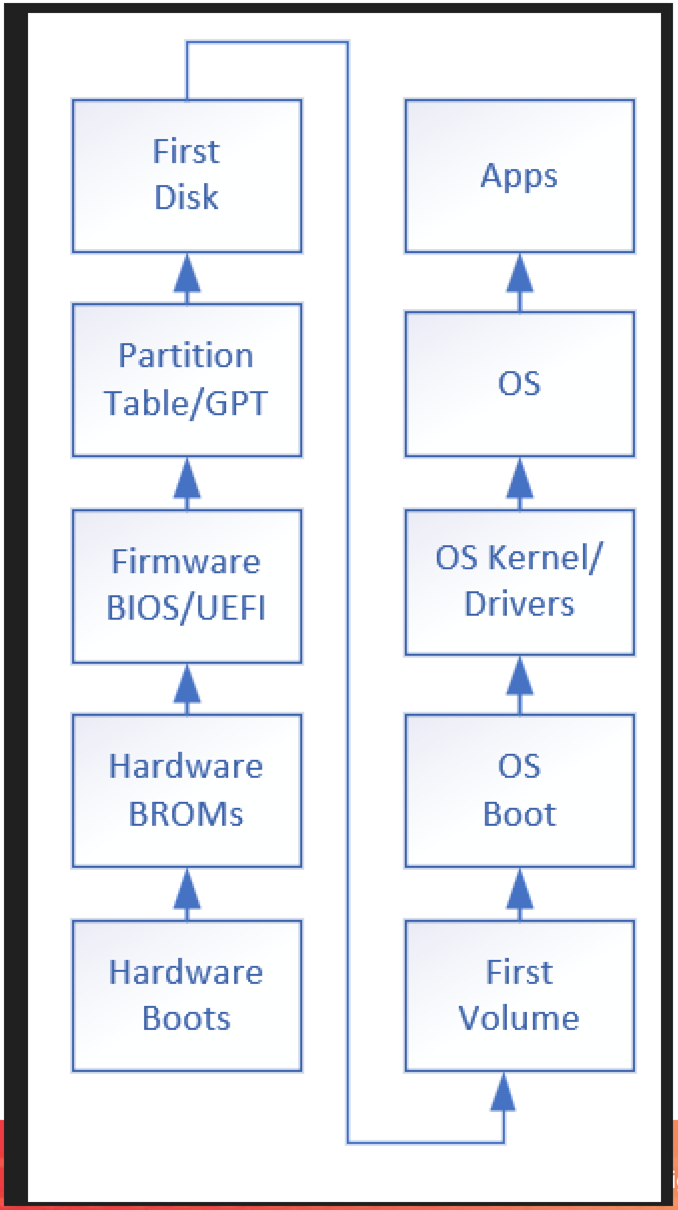


```
Dell Inc.                                          Aptio Setup Ut
  Main   Advanced   Security   Boot   Exit

  Boot List Option                       [UEFI]
  File Browser Add Boot Option
  File Browser Del Boot Option
  Secure Boot                            [Enabled]
  Legacy Option ROMs                     [Disabled]
  Attempt Legacy Boot                    [Disabled]

  Boot Option Priorities
  Boot Option #1                         [Windows Boot Manager]
  Boot Option #2                         [Onboard NIC (IPV4)]
  Boot Option #3                         ── Secure Boot ──
                                         Disabled
                                         Enabled
```

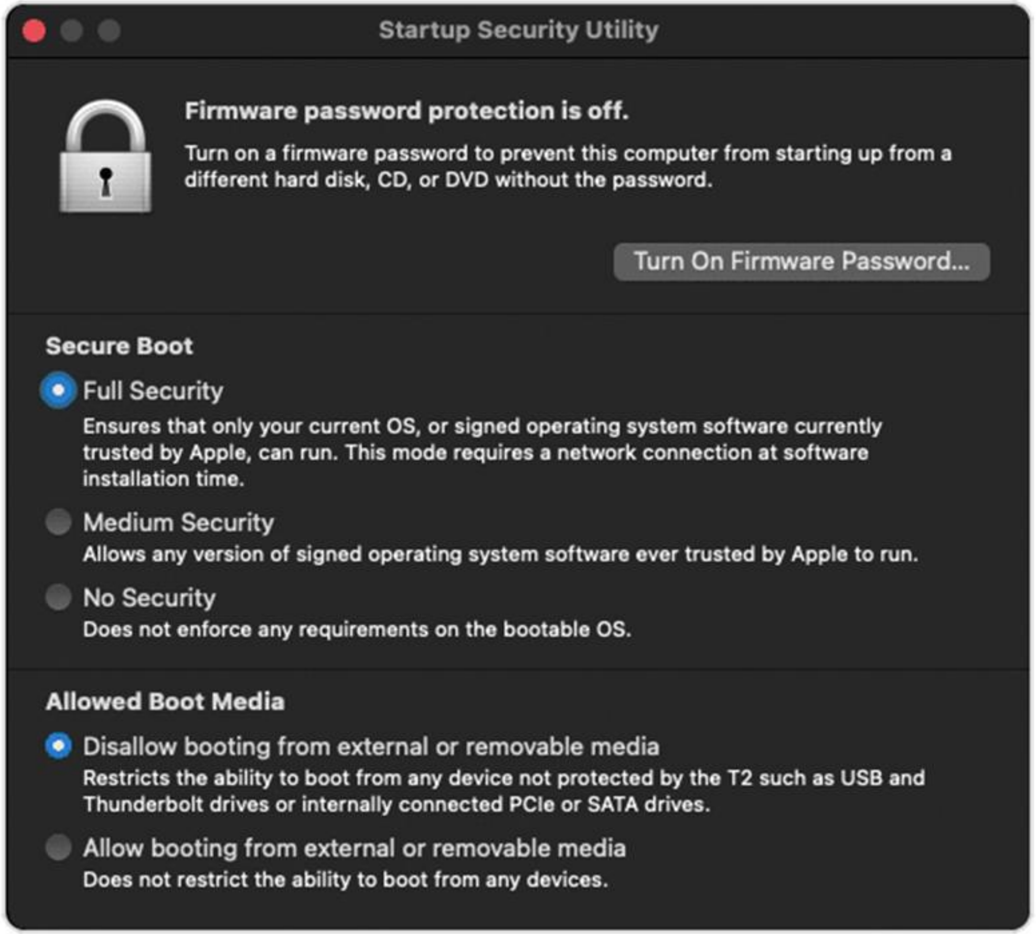
top-password.com



The Full Solution

Trusted Hardware Boot

- Hardware Boot
- Hardware Secure Boot
- BIOS/UEFI protected
- Secure hand off to the OS



Startup Security Utility

Firmware password protection is off.

Turn on a firmware password to prevent this computer from starting up from a different hard disk, CD, or DVD without the password.

Turn On Firmware Password...

Secure Boot

● Full Security
Ensures that only your current OS, or signed operating system software currently trusted by Apple, can run. This mode requires a network connection at software installation time.

○ Medium Security
Allows any version of signed operating system software ever trusted by Apple to run.

○ No Security
Does not enforce any requirements on the bootable OS.

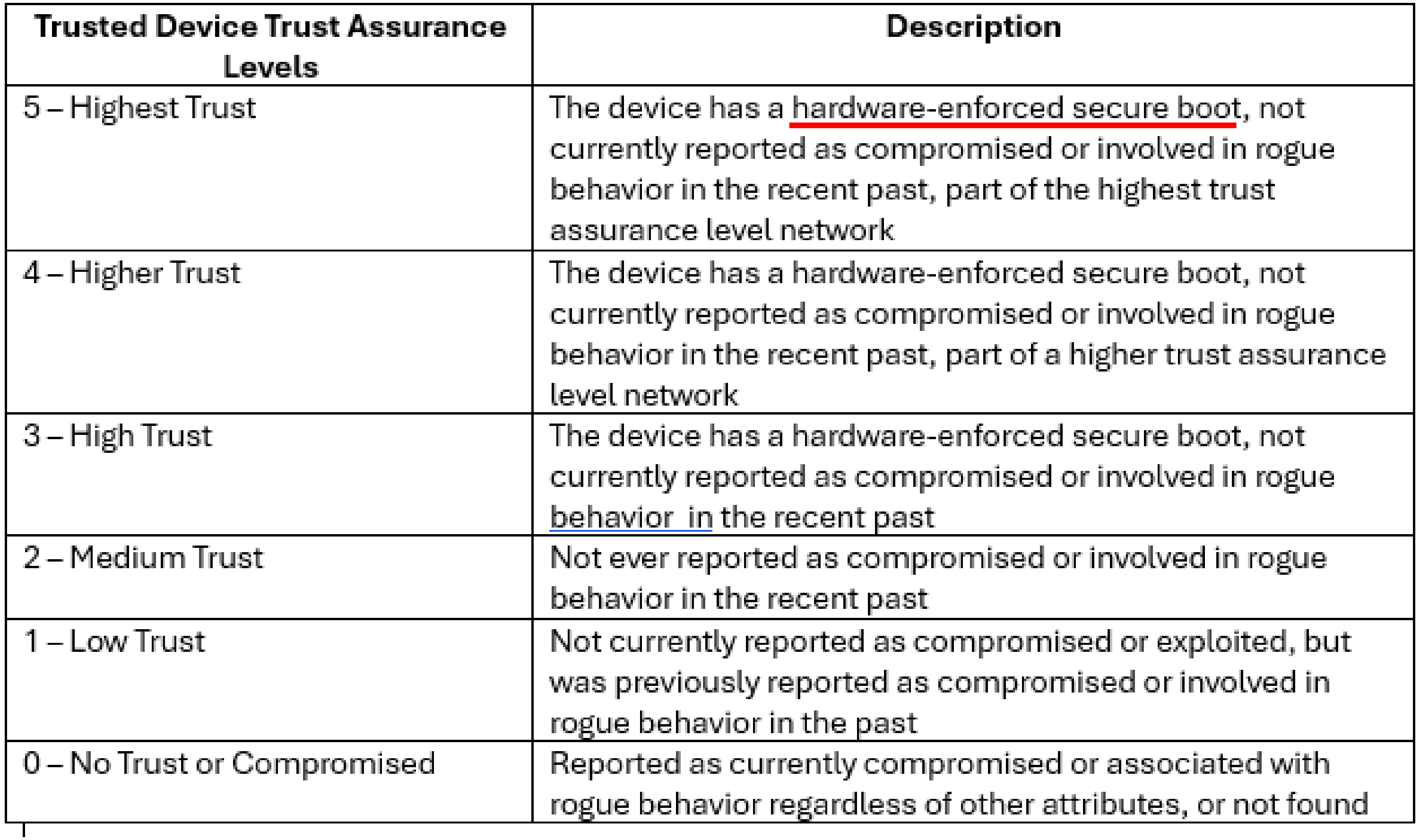
Allowed Boot Media

● Disallow booting from external or removable media
Restricts the ability to boot from any device not protected by the T2 such as USB and Thunderbolt drives or internally connected PCIe or SATA drives.

○ Allow booting from external or removable media
Does not restrict the ability to boot from any devices.

The Full Solution

Trusted Device



Trusted Device Trust Assurance Levels	Description
5 – Highest Trust	The device has a hardware-enforced secure boot, not currently reported as compromised or involved in rogue behavior in the recent past, part of the highest trust assurance level network
4 – Higher Trust	The device has a hardware-enforced secure boot, not currently reported as compromised or involved in rogue behavior in the recent past, part of a higher trust assurance level network
3 – High Trust	The device has a hardware-enforced secure boot, not currently reported as compromised or involved in rogue behavior in the recent past
2 – Medium Trust	Not ever reported as compromised or involved in rogue behavior in the recent past
1 – Low Trust	Not currently reported as compromised or exploited, but was previously reported as compromised or involved in rogue behavior in the past
0 – No Trust or Compromised	Reported as currently compromised or associated with rogue behavior regardless of other attributes, or not found

Hardware-enforced secure device boot

The Full Solution

Trusted Verified Device Identities

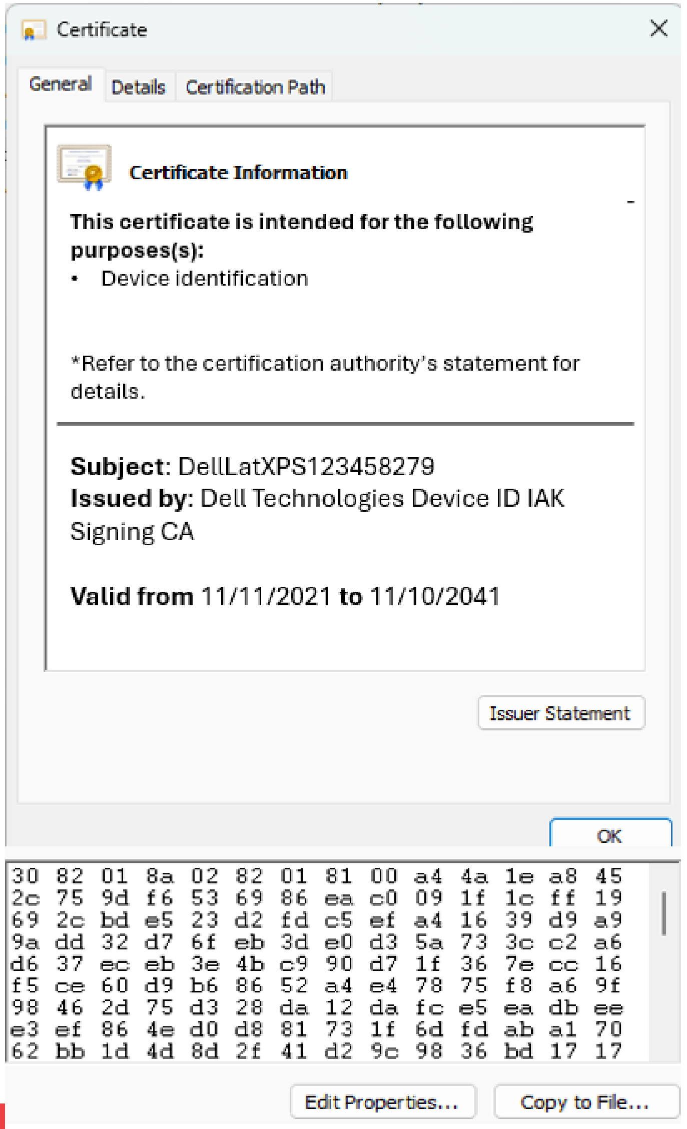
- We need to confirm that users are coming from known trusted devices that they previously used;
- And if not, higher risk, ask for more authentication
- This is already done on the major websites, with varying levels of accuracy

The Full Solution

Trusted Verified Device Identities

Best Method

- Device ID digital certificate
- Created by developer and,
- Stored on TPM-like chip
- Can be securely queried by using API



Certificate Information

This certificate is intended for the following purposes(s):

- Device identification

*Refer to the certification authority's statement for details.

Subject: DellLatXPS123458279
Issued by: Dell Technologies Device ID IAK Signing CA

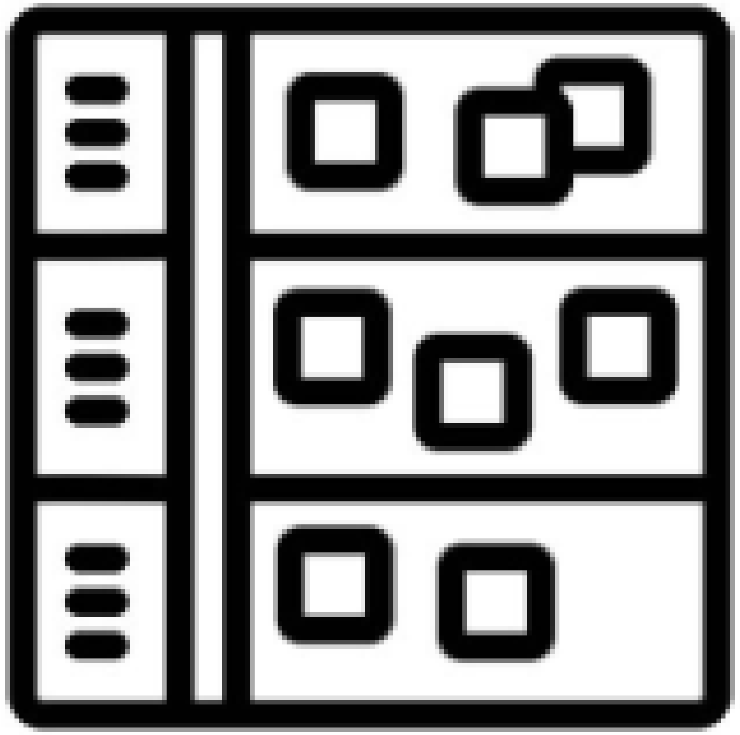
Valid from 11/11/2021 **to** 11/10/2041

```
30 82 01 8a 02 82 01 81 00 a4 4a 1e a8 45
2c 75 9d f6 53 69 86 ea c0 09 1f 1c ff 19
69 2c bd e5 23 d2 fd c5 ef a4 16 39 d9 a9
9a dd 32 d7 6f eb 3d e0 d3 5a 73 3c c2 a6
d6 37 ec eb 3e 4b c9 90 d7 1f 36 7e cc 16
f5 ce 60 d9 b6 86 52 a4 e4 78 75 f8 a6 9f
98 46 2d 75 d3 28 da 12 da fc e5 ea db ee
e3 ef 86 4e d0 d8 81 73 1f 6d fd ab a1 70
62 bb 1d 4d 8d 2f 41 d2 9c 98 36 bd 17 17
```

Hypervisor?

Definition

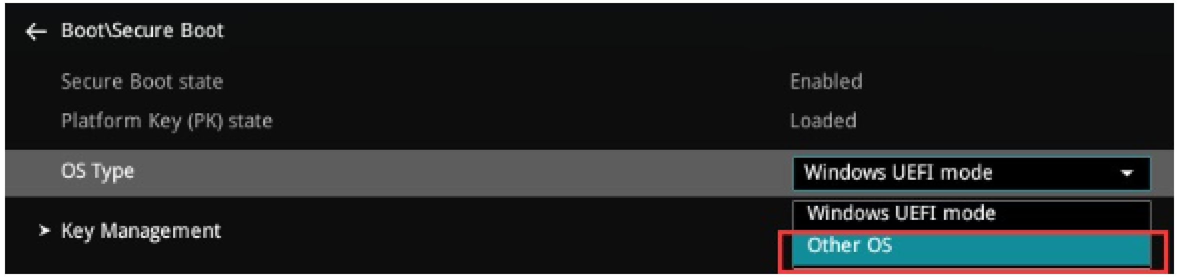
- Special area of memory set aside and protected
  - For VMs, booting, OS, programs, data, etc.
- Is protected from outside interference
- Can be software- or hardware-enforced
  - Hardware-enforced is better



The Full Solution

Trusted OS

- Starts with hardware chip
- OS Secure Boot
- OS Memory protections



← Boot\Secure Boot

Secure Boot state: Enabled

Platform Key (PK) state: Loaded

OS Type: Windows UEFI mode

Here are some of the TPM PCRs that Windows uses when it boots:

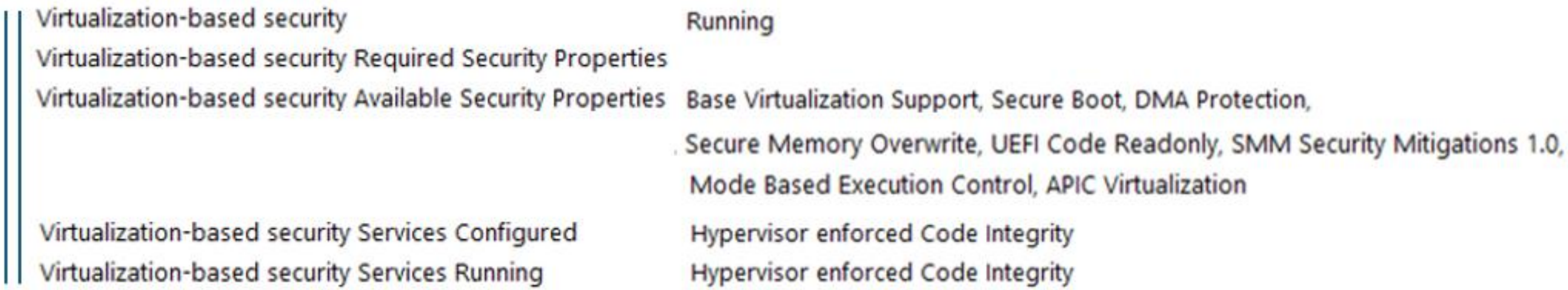
- PCR 0: Core root-of-trust for measurement, UEFI boot and run-time services, UEFI drivers embedded in system ROM, ACPI static tables, embedded SMM code, and BIOS code
- PCR 1: Platform and motherboard configuration and data. It also hands off tables and UEFI variables that affect system configuration
- PCR 2: Option ROM code
- PCR 3: Option ROM data and configuration
- PCR 4: Master boot record (MBR) code or code from other boot devices
- PCR 5: Master boot record (MBR) partition table. Various UEFI variables and the GUID partition table (GPT)
- PCR 6: State transition and wake events
- PCR 7: Computer manufacturer-specific (i.e., Microsoft will use this)
- PCR 8: NTFS boot sector
- PCR 9: NTFS boot block
- PCR 10: Boot manager
- PCR 11: BitLocker access control

The Full Solution

Trusted OS – Good

- Hardware-enforced hypervisor security domain isolation

Example: Microsoft Windows



Virtualization-based security	Running
Virtualization-based security Required Security Properties	
Virtualization-based security Available Security Properties	Base Virtualization Support, Secure Boot, DMA Protection, Secure Memory Overwrite, UEFI Code Readonly, SMM Security Mitigations 1.0, Mode Based Execution Control, APIC Virtualization
Virtualization-based security Services Configured	Hypervisor enforced Code Integrity
Virtualization-based security Services Running	Hypervisor enforced Code Integrity

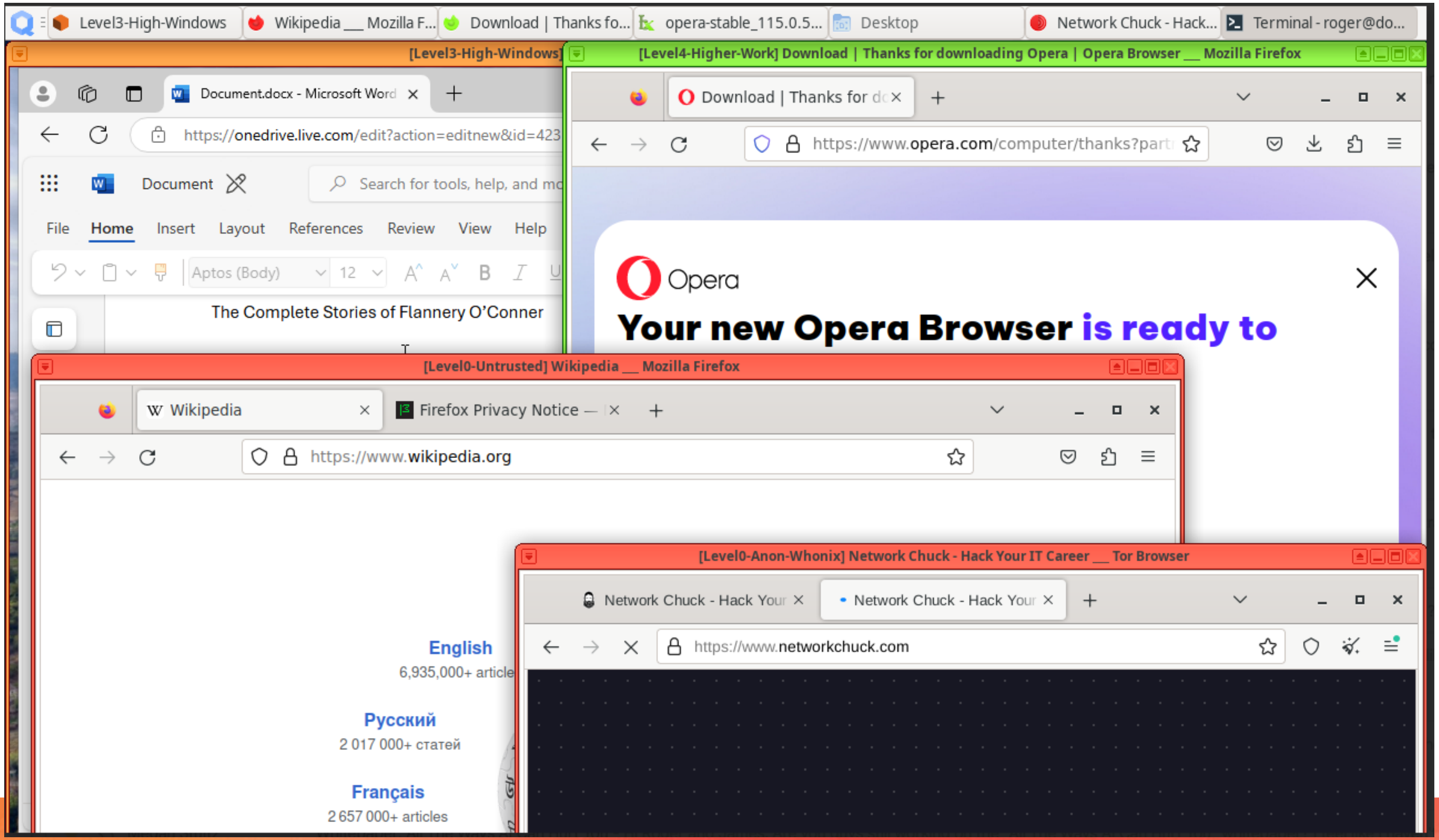
MSInfo32.exe

The Full Solution

Trusted OS – The Best

- Hardware-enforced hypervisor security domain isolation (Qubes OS)

Qubes-os.org



Level3-High-Windows
Wikipedia __ Mozilla F...
Download | Thanks fo...
opera-stable_115.0.5...
Desktop
Network Chuck - Hack...
Terminal - roger@do...
[Level3-High-Windows]
Document.docx - Microsoft Word
https://onedrive.live.com/edit?action=editnew&id=423
Document
Search for tools, help, and mo
File
Home
Insert
Layout
References
Review
View
Help
Aptos (Body)
12
B
I
U
[Level4-Higher-Work] Download | Thanks for downloading Opera | Opera Browser __ Mozilla Firefox
Download | Thanks for d
https://www.opera.com/computer/thanks?part
Opera
[Level0-Untrusted] Wikipedia __ Mozilla Firefox
Wikipedia
Firefox Privacy Notice —
https://www.wikipedia.org
[Level0-Anon-Whonix] Network Chuck - Hack Your IT Career __ Tor Browser
Network Chuck - Hack Your
Network Chuck - Hack Your
https://www.networkchuck.com

The Complete Stories of Flannery O'Conner

Your new Opera Browser is ready to

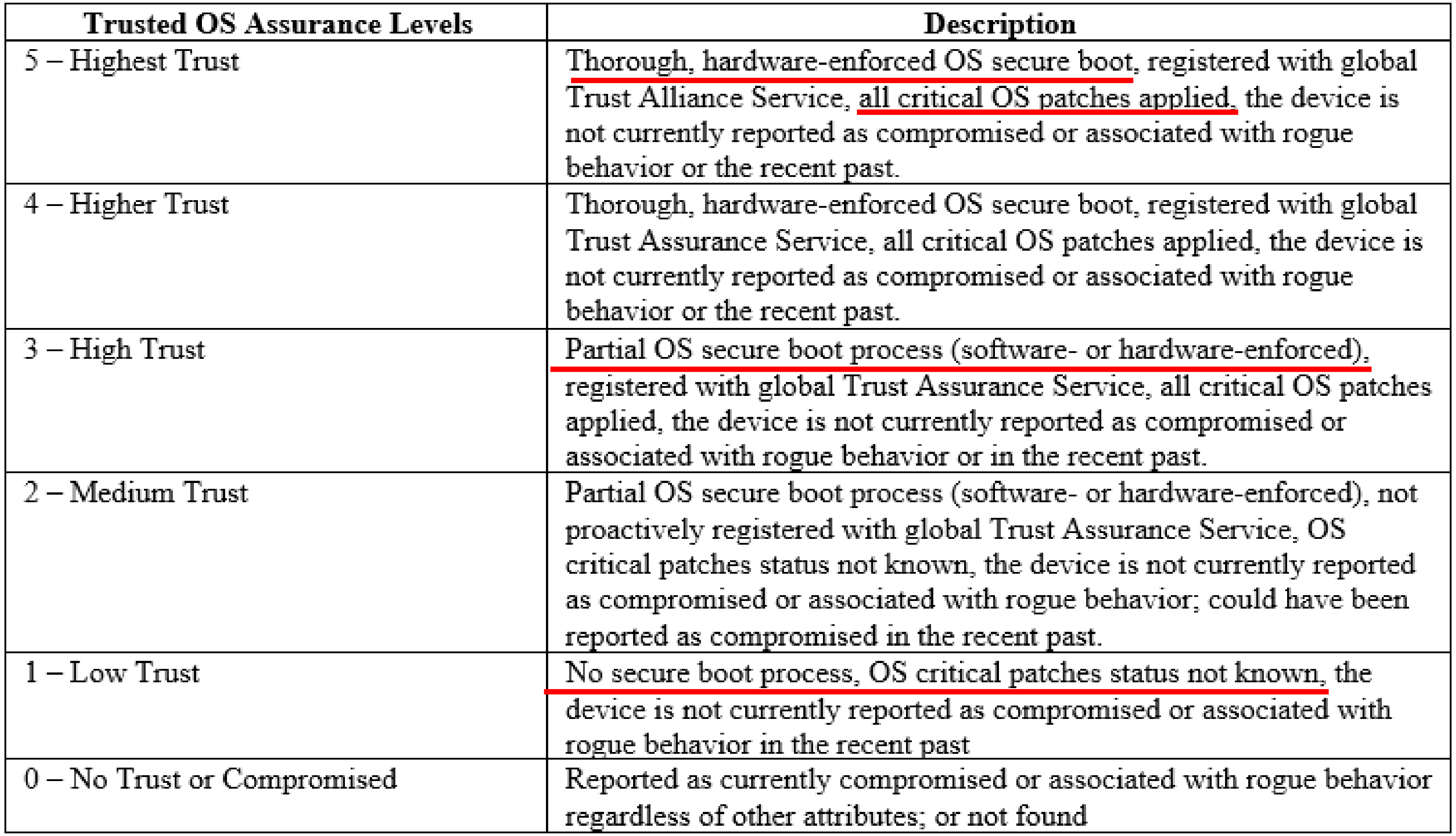
English
6,935,000+ article

Русский
2 017 000+ статей

Français
2 657 000+ articles

The Full Solution

Trusted OS



Trusted OS Assurance Levels	Description
5 – Highest Trust	Thorough, hardware-enforced OS secure boot, registered with global Trust Alliance Service, all critical OS patches applied, the device is not currently reported as compromised or associated with rogue behavior or the recent past.
4 – Higher Trust	Thorough, hardware-enforced OS secure boot, registered with global Trust Assurance Service, all critical OS patches applied, the device is not currently reported as compromised or associated with rogue behavior or the recent past.
3 – High Trust	Partial OS secure boot process (software- or hardware-enforced), registered with global Trust Assurance Service, all critical OS patches applied, the device is not currently reported as compromised or associated with rogue behavior or in the recent past.
2 – Medium Trust	Partial OS secure boot process (software- or hardware-enforced), not proactively registered with global Trust Assurance Service, OS critical patches status not known, the device is not currently reported as compromised or associated with rogue behavior; could have been reported as compromised in the recent past.
1 – Low Trust	No secure boot process, OS critical patches status not known, the device is not currently reported as compromised or associated with rogue behavior in the recent past
0 – No Trust or Compromised	Reported as currently compromised or associated with rogue behavior regardless of other attributes; or not found

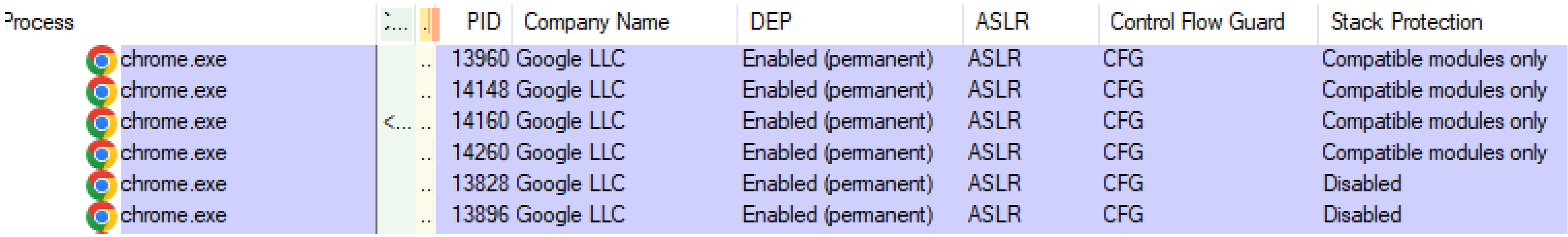
Hardware-enforced OS secure boot, fully patched

Hardware-or software-enforced Partial OS secure boot

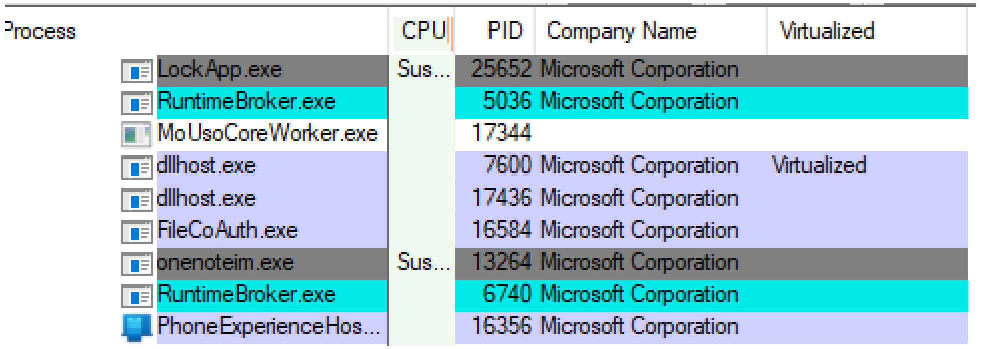
The Full Solution

Trusted Apps

- Global Unique Application Identifier
- Digitally Signed
- Securely Code
- Secure Defaults
- Self-Checking Integrity
- Application Memory Protections
- Securely Configured
- Application Control
- Security-Bound Cookies



Process	:...	.	PID	Company Name	DEP	ASLR	Control Flow Guard	Stack Protection
chrome.exe		..	13960	Google LLC	Enabled (permanent)	ASLR	CFG	Compatible modules only
chrome.exe		..	14148	Google LLC	Enabled (permanent)	ASLR	CFG	Compatible modules only
chrome.exe	<...	..	14160	Google LLC	Enabled (permanent)	ASLR	CFG	Compatible modules only
chrome.exe		..	14260	Google LLC	Enabled (permanent)	ASLR	CFG	Compatible modules only
chrome.exe		..	13828	Google LLC	Enabled (permanent)	ASLR	CFG	Disabled
chrome.exe		..	13896	Google LLC	Enabled (permanent)	ASLR	CFG	Disabled

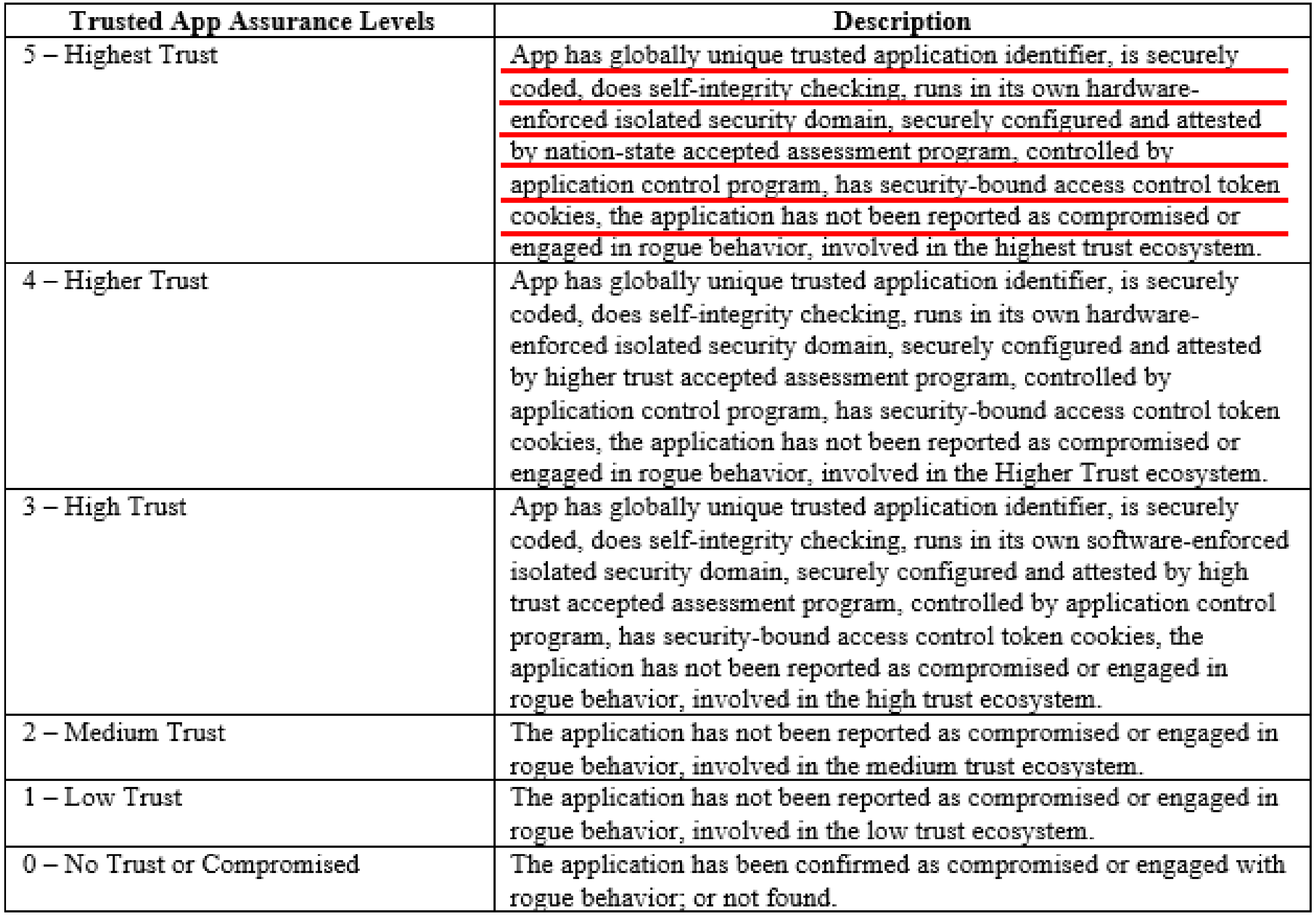


Process	CPU	PID	Company Name	Virtualized
LockApp.exe	Sus...	25652	Microsoft Corporation	
RuntimeBroker.exe		5036	Microsoft Corporation	
MoUsoCoreWorker.exe		17344		
dllhost.exe		7600	Microsoft Corporation	Virtualized
dllhost.exe		17436	Microsoft Corporation	
FileCoAuth.exe		16584	Microsoft Corporation	
onenoteim.exe	Sus...	13264	Microsoft Corporation	
RuntimeBroker.exe		6740	Microsoft Corporation	
PhoneExperienceHos...		16356	Microsoft Corporation	

Images from Process Explorer

The Full Solution

Trusted Apps



Trusted App Assurance Levels	Description
5 – Highest Trust	App has globally unique trusted application identifier, is securely coded, does self-integrity checking, runs in its own hardware-enforced isolated security domain, securely configured and attested by nation-state accepted assessment program, controlled by application control program, has security-bound access control token cookies, the application has not been reported as compromised or engaged in rogue behavior, involved in the highest trust ecosystem.
4 – Higher Trust	App has globally unique trusted application identifier, is securely coded, does self-integrity checking, runs in its own hardware-enforced isolated security domain, securely configured and attested by higher trust accepted assessment program, controlled by application control program, has security-bound access control token cookies, the application has not been reported as compromised or engaged in rogue behavior, involved in the Higher Trust ecosystem.
3 – High Trust	App has globally unique trusted application identifier, is securely coded, does self-integrity checking, runs in its own software-enforced isolated security domain, securely configured and attested by high trust accepted assessment program, controlled by application control program, has security-bound access control token cookies, the application has not been reported as compromised or engaged in rogue behavior, involved in the high trust ecosystem.
2 – Medium Trust	The application has not been reported as compromised or engaged in rogue behavior, involved in the medium trust ecosystem.
1 – Low Trust	The application has not been reported as compromised or engaged in rogue behavior, involved in the low trust ecosystem.
0 – No Trust or Compromised	The application has been confirmed as compromised or engaged with rogue behavior; or not found.

The Full Solution

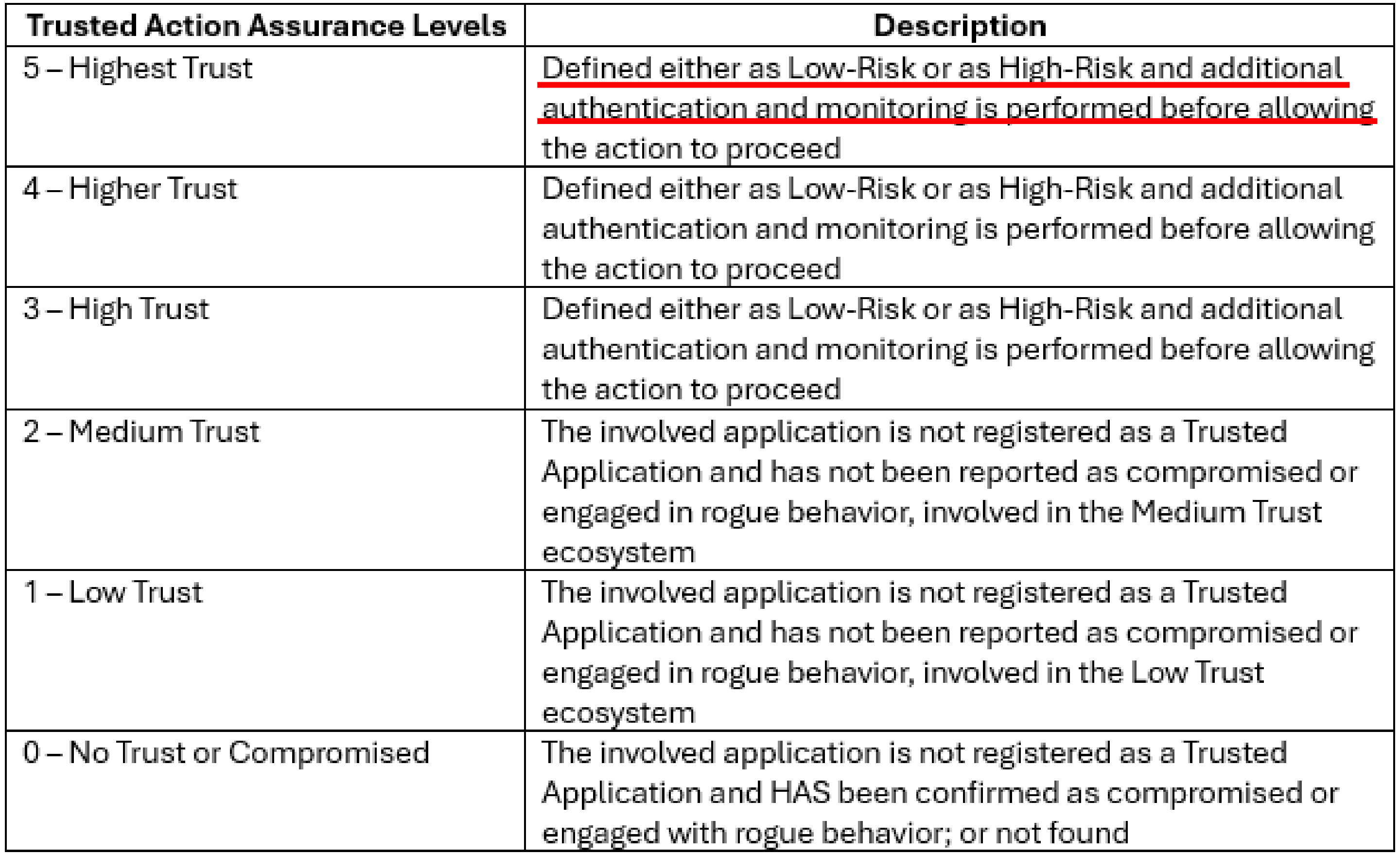
Trusted Actions

- Different actions have different levels of trust and require different levels of authentication
- Defined by app, site, or service provider
- Checking your bank balance is a low- to medium-risk transaction
- Transferring your entire bank account balance to a new Russian bank you've never dealt with before is a high-risk transaction
- Applications and services should define transactional risk
- And ask for additional authentication for high-risk transactions
  - Called *dynamic authentication*

This is a big part of "zero trust"

The Full Solution

Trusted Actions



Trusted Action Assurance Levels	Description
5 – Highest Trust	Defined either as Low-Risk or as High-Risk and additional authentication and monitoring is performed before allowing the action to proceed
4 – Higher Trust	Defined either as Low-Risk or as High-Risk and additional authentication and monitoring is performed before allowing the action to proceed
3 – High Trust	Defined either as Low-Risk or as High-Risk and additional authentication and monitoring is performed before allowing the action to proceed
2 – Medium Trust	The involved application is not registered as a Trusted Application and has not been reported as compromised or engaged in rogue behavior, involved in the Medium Trust ecosystem
1 – Low Trust	The involved application is not registered as a Trusted Application and has not been reported as compromised or engaged in rogue behavior, involved in the Low Trust ecosystem
0 – No Trust or Compromised	The involved application is not registered as a Trusted Application and HAS been confirmed as compromised or engaged with rogue behavior; or not found

Trusted app with defined trusted actions

The Full Solution

Trusted Networks

- Data Integrity and Security
  - VPN, HTTPS, etc.
- Node compliance
  - Is it fully patched, securely configured, etc.
- Is node known to be safe
- Is network known to be safe?

There are

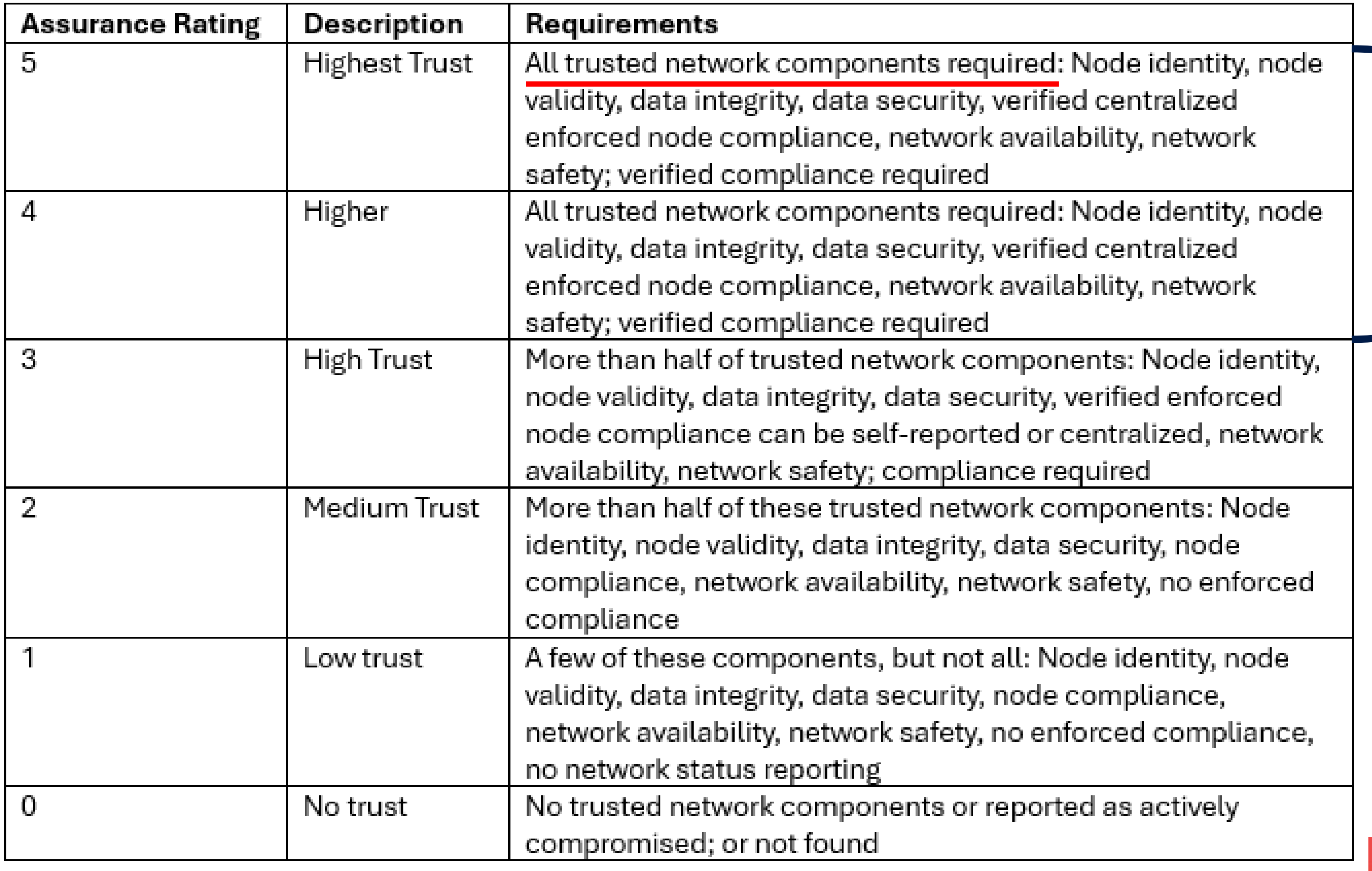
Good networks

and

Bad networks

The Full Solution

Trusted Networks



Assurance Rating	Description	Requirements
5	Highest Trust	All trusted network components required: Node identity, node validity, data integrity, data security, verified centralized enforced node compliance, network availability, network safety; verified compliance required
4	Higher	All trusted network components required: Node identity, node validity, data integrity, data security, verified centralized enforced node compliance, network availability, network safety; verified compliance required
3	High Trust	More than half of trusted network components: Node identity, node validity, data integrity, data security, verified enforced node compliance can be self-reported or centralized, network availability, network safety; compliance required
2	Medium Trust	More than half of these trusted network components: Node identity, node validity, data integrity, data security, node compliance, network availability, network safety, no enforced compliance
1	Low trust	A few of these components, but not all: Node identity, node validity, data integrity, data security, node compliance, network availability, network safety, no enforced compliance, no network status reporting
0	No trust	No trusted network components or reported as actively compromised; or not found

Fully Trusted network

The Full Solution

Trust Assurance Service

- Local Trust Assurance Service
- Global Trust Assurance Service

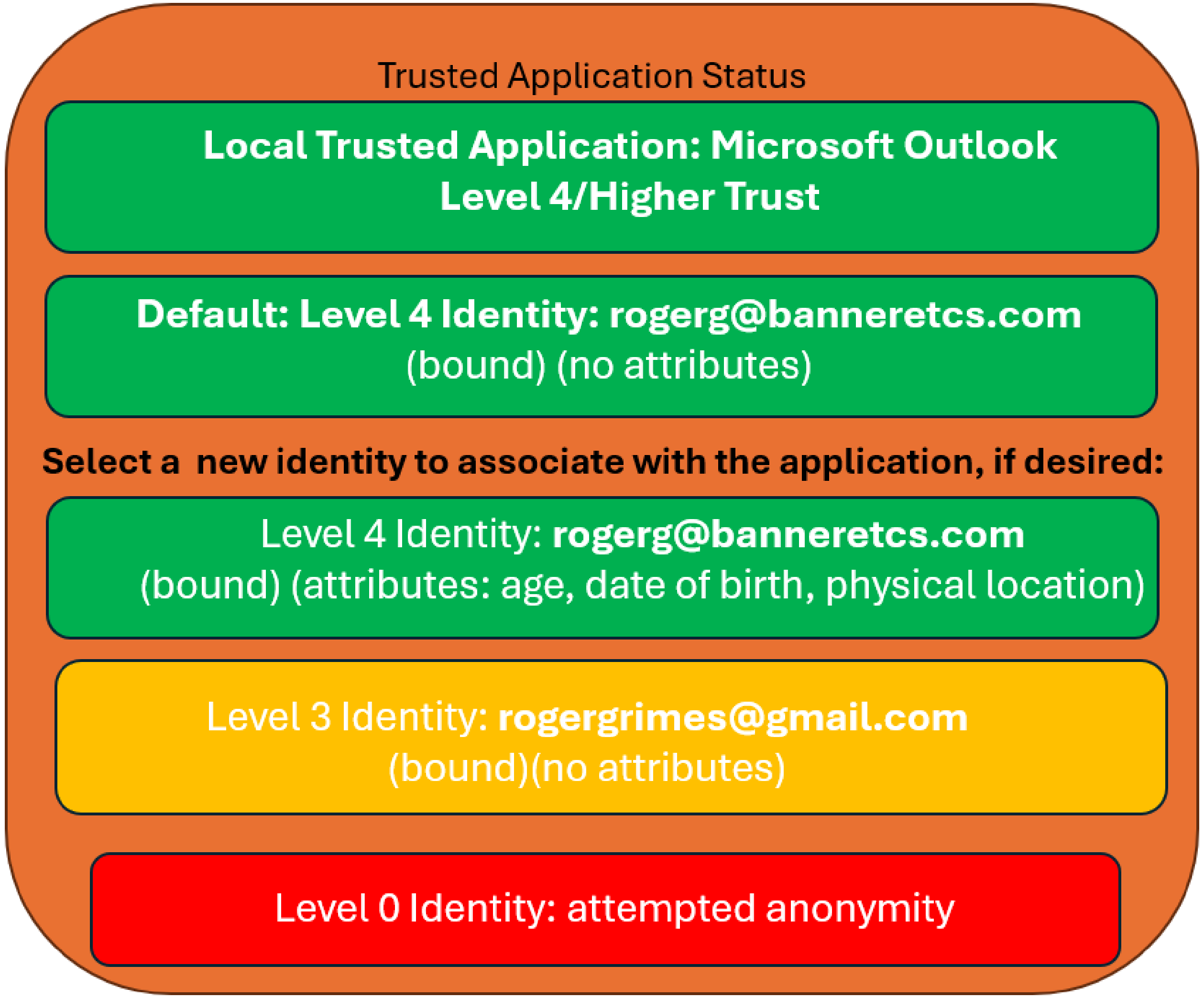
The Full Solution

Local Trust Assurance Service

- Interfaces with the user
- Manages the user's own trusted identities, personas, and attributes
- Allows the user to select the identities, personas, and attributes for particular applications/sites/services, etc.
- Helps set up new connections
- Handles new remote requests from new and existing connections
- Interfaces with global Internet Trust Assurance Service

The Full Solution

Local Trust Assurance Service (con’t)



Trusted Application Status

Local Trusted Application: Microsoft Outlook
Level 4/Higher Trust

Default: Level 4 Identity: rogerg@banneretcs.com
(bound) (no attributes)

Select a new identity to associate with the application, if desired:

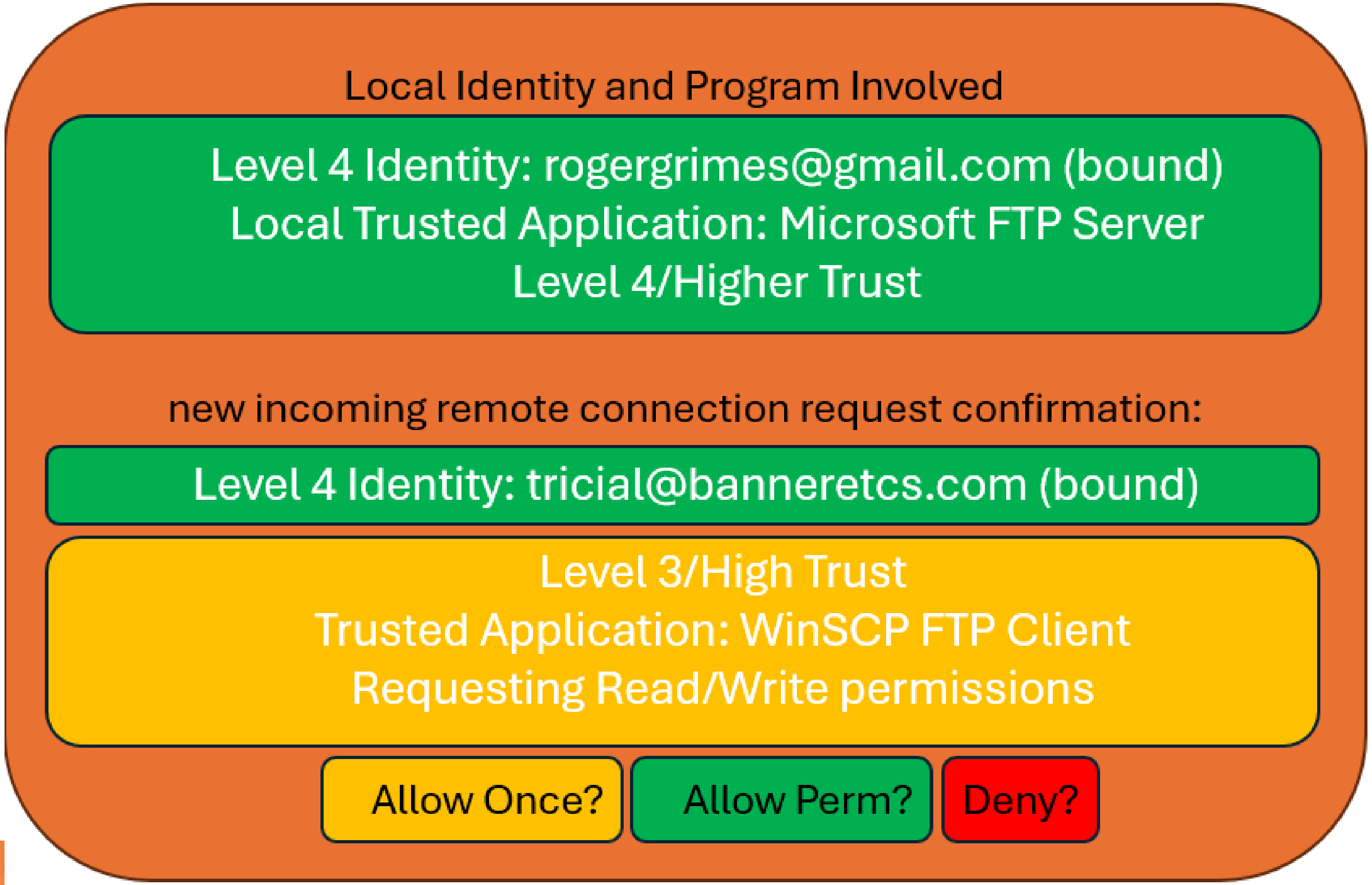
Level 4 Identity: **rogerg@banneretcs.com**
(bound) (attributes: age, date of birth, physical location)

Level 3 Identity: **rogergrimes@gmail.com**
(bound)(no attributes)

Level 0 Identity: attempted anonymity

The Full Solution

Local Trust Assurance Service (con’t)



Local Identity and Program Involved

Level 4 Identity: rogergrimes@gmail.com (bound)
Local Trusted Application: Microsoft FTP Server
Level 4/Higher Trust

new incoming remote connection request confirmation:

Level 4 Identity: tricial@banneretcs.com (bound)

Level 3/High Trust
Trusted Application: WinSCP FTP Client
Requesting Read/Write permissions

The Full Solution

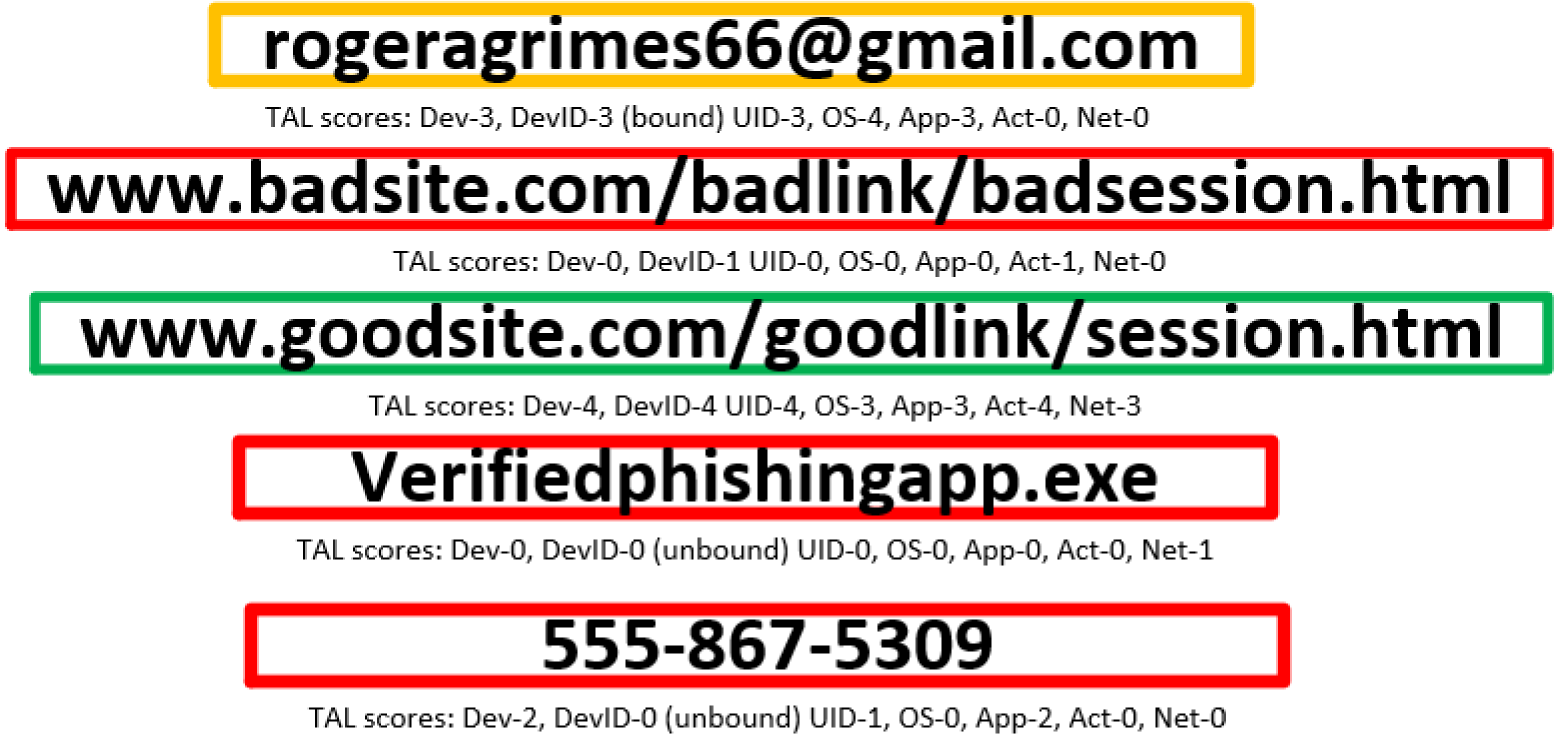
Local Trust Assurance Service (con’t)

- Automatically submits email addresses, files, URLs, phone numbers, and other content items to the global Trust Assurance Service for trustworthiness when a user views them
- Allows user to easily and quickly report suspected maliciousness

The Full Solution

Local Trust Assurance Service

Example of Verified Submitted Contact Info



rogeragrimes66@gmail.com

TAL scores: Dev-3, DevID-3 (bound) UID-3, OS-4, App-3, Act-0, Net-0

www.badsite.com/badlink/badsession.html

TAL scores: Dev-0, DevID-1 UID-0, OS-0, App-0, Act-1, Net-0

www.goodsite.com/goodlink/session.html

TAL scores: Dev-4, DevID-4 UID-4, OS-3, App-3, Act-4, Net-3

Verifiedphishingapp.exe

TAL scores: Dev-0, DevID-0 (unbound) UID-0, OS-0, App-0, Act-0, Net-1

555-867-5309

TAL scores: Dev-2, DevID-0 (unbound) UID-1, OS-0, App-2, Act-0, Net-0

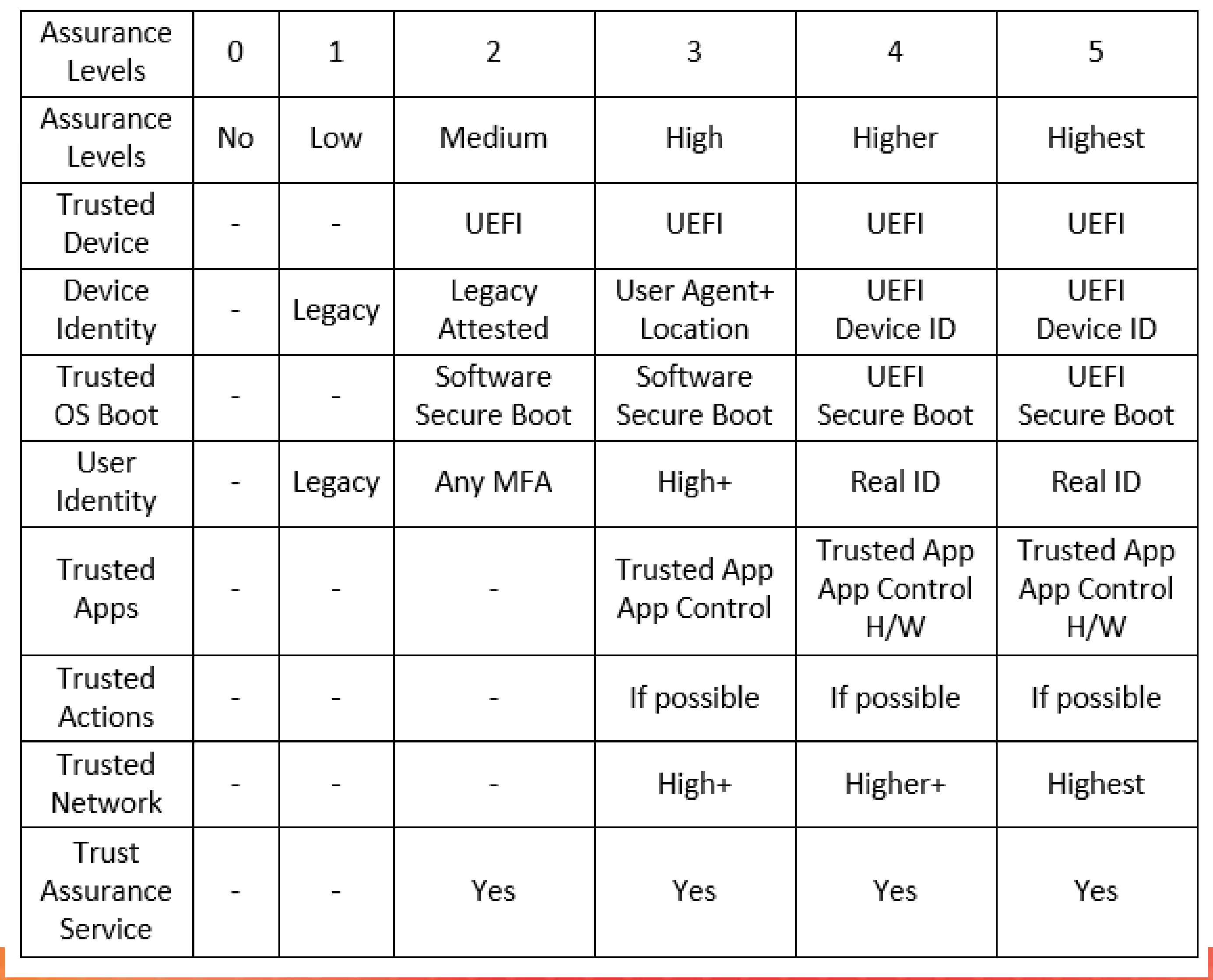
The Full Solution

Global Trust Assurance Service

- Fully-funded, DNS-like, global service that handles centralized duties of Trust Assurance Service
- Investigates submitted links and content
- Has global Allow List
- Has global Block List

Fed by
Cybersecurity Vendors
And
Own Data

The Full Trust Stack



Assurance Levels	0	1	2	3	4	5
Assurance Levels	No	Low	Medium	High	Higher	Highest
Trusted Device	-	-	UEFI	UEFI	UEFI	UEFI
Device Identity	-	Legacy	Legacy Attested	User Agent+ Location	UEFI Device ID	UEFI Device ID
Trusted OS Boot	-	-	Software Secure Boot	Software Secure Boot	UEFI Secure Boot	UEFI Secure Boot
User Identity	-	Legacy	Any MFA	High+	Real ID	Real ID
Trusted Apps	-	-	-	Trusted App App Control	Trusted App App Control H/W	Trusted App App Control H/W
Trusted Actions	-	-	-	If possible	If possible	If possible
Trusted Network	-	-	-	High+	Higher+	Highest
Trust Assurance Service	-	-	Yes	Yes	Yes	Yes

The Solution

Verified Trust

- Are you who you say you are?

Answer: Yes, I’m Roger A. Grimes, Real ID, Trust Assurance Level 4

- Is that program, link, or content what it says it is?

Answer: Yes, and not currently or previously marked as malicious

Agenda

KnowBe4

- How Bad Is It?
- The Main Underlying Problem
- The Solution
- Other Needed Solutions

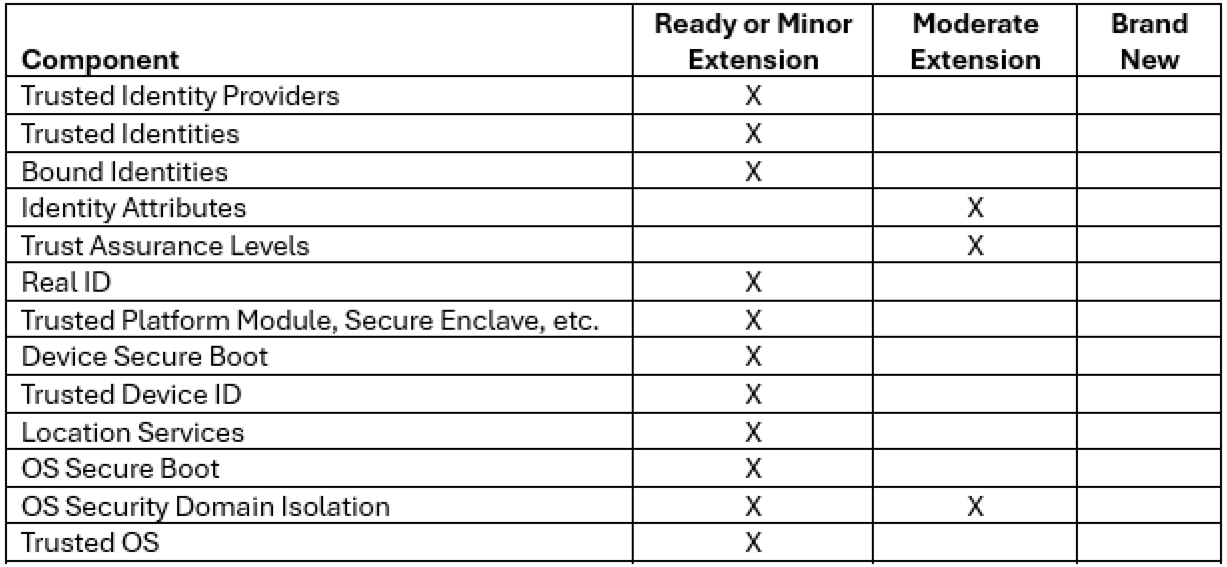
Other Needed Solutions

Other Big Solutions Needed

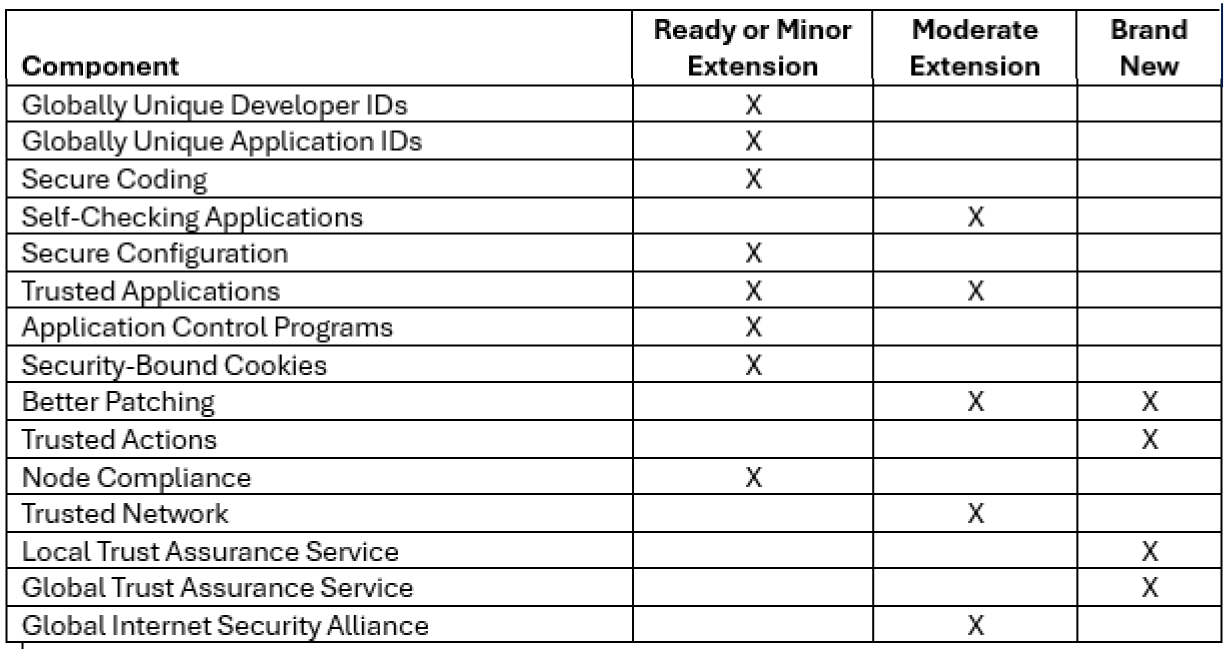
- **More Secure Coding**
  - Train Developers in Secure Coding
  - Require Developers to have Secure Coding Skills

- **Better, Faster Patching**
  - More auto-patching without end-user interaction
  - Faster patching
  - Easier reversion, in case of error

Not Far Fetched – Most Tech Already Exists



Component	Ready or Minor Extension	Moderate Extension	Brand New
Trusted Identity Providers	X		
Trusted Identities	X		
Bound Identities	X		
Identity Attributes		X	
Trust Assurance Levels		X	
Real ID	X		
Trusted Platform Module, Secure Enclave, etc.	X		
Device Secure Boot	X		
Trusted Device ID	X		
Location Services	X		
OS Secure Boot	X		
OS Security Domain Isolation	X	X	
Trusted OS	X		



Component	Ready or Minor Extension	Moderate Extension	Brand New
Globally Unique Developer IDs	X		
Globally Unique Application IDs	X		
Secure Coding	X		
Self-Checking Applications		X	
Secure Configuration	X		
Trusted Applications	X	X	
Application Control Programs	X		
Security-Bound Cookies	X		
Better Patching		X	X
Trusted Actions			X
Node Compliance	X		
Trusted Network		X	
Local Trust Assurance Service			X
Global Trust Assurance Service			X
Global Internet Security Alliance		X	

Maybe my solution isn’t the right one

But we need something different than what we have already been trying

Demand better security solutions

Participate in groups to make better security solutions

Questions?

Roger A. Grimes– Data-Driven Defense Evangelist, KnowBe4
e: rogerg@knowbe4.com

Twitter: @RogerAGrimes
LinkedIn: https://www.linkedin.com/in/rogeragrimes/
Mastodon: https://infosec.exchange/@rogeragrimes
YouTube: @CyberSecWTFRants
rogeragrimes@bsky.social