



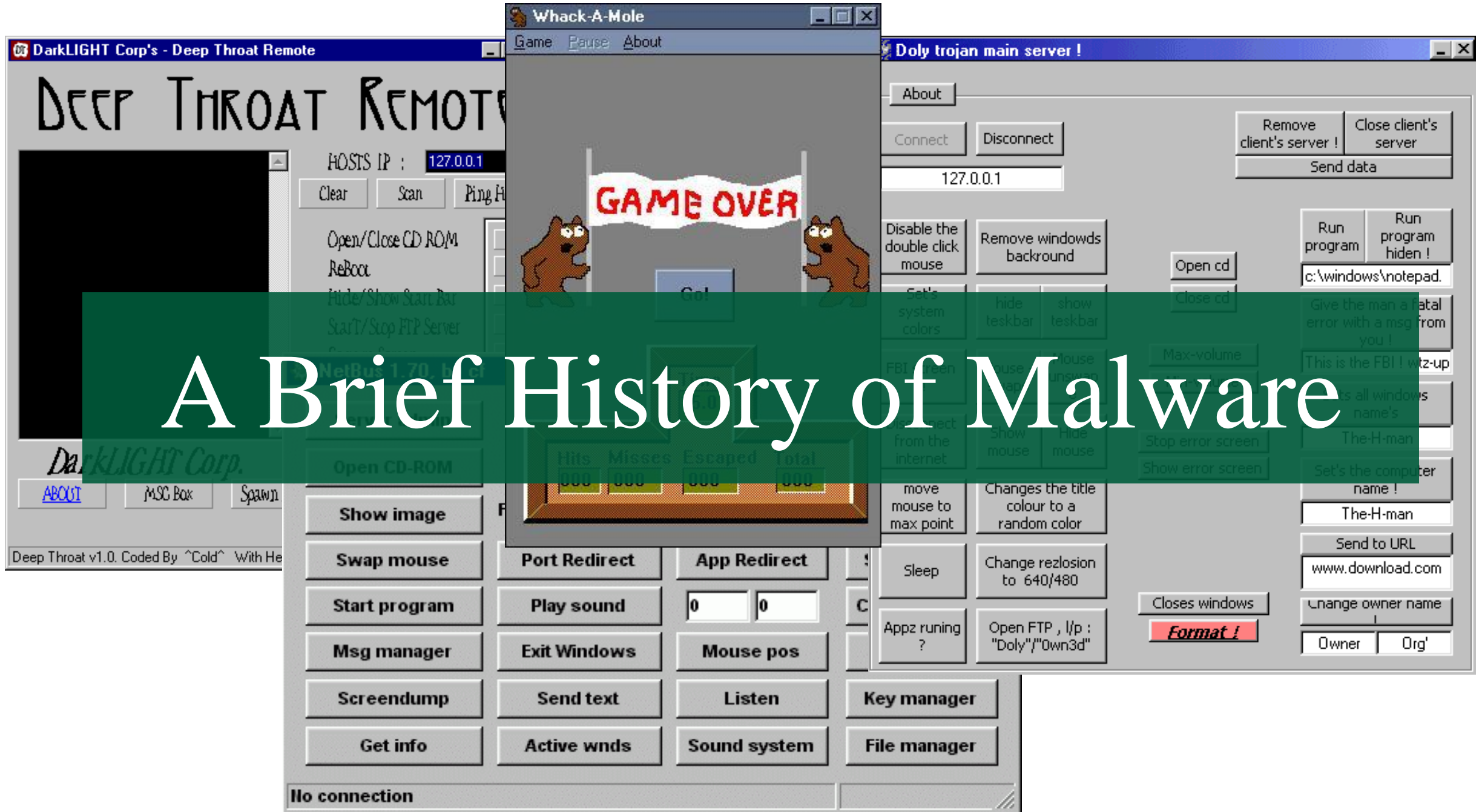
Why is your IT security team so interested in your test system?

NI Connect 2023

Steve Summers

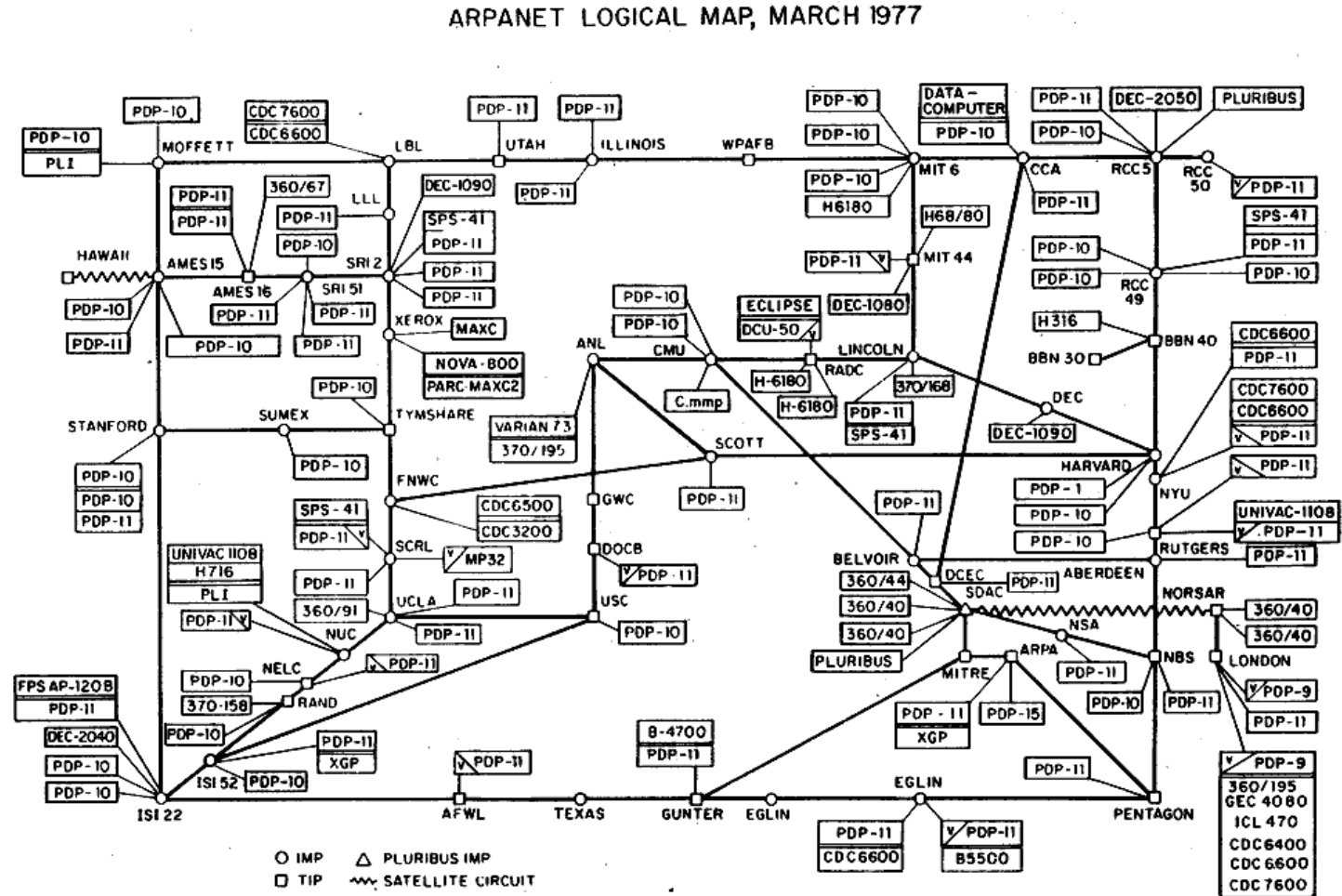
Security Lead, ADG Business Unit

A Brief History of Malware



First computer worm

- Self-replicating program
- Spread on ARPANET
- Named after a Scooby-Doo villain: The Creeper
- “Reaper” created to remove The Creeper.



I'M THE CREEPER. CATCH ME IF YOU CAN!

First “wild” virus

- Written by 15-year-old high school student
- Released as a joke
- Infected Apple II OS machines
- Spread on boot sector of floppy disks

1982



AIDS Trojan

- First Ransomware attack
- Replaced AUTEEXEC.BAT
- After 90 boots, hid directories and encrypted files
- \$189 payment sent to Panama
- 1989 Fix disk sent to user
- Created by Harvard professor
- Proceeds benefitted AIDS research (maybe?)

Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation. Complete the INVOICE and attach payment for the lease option of your choice. If you don't use the printed INVOICE, then be sure to refer to the important reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

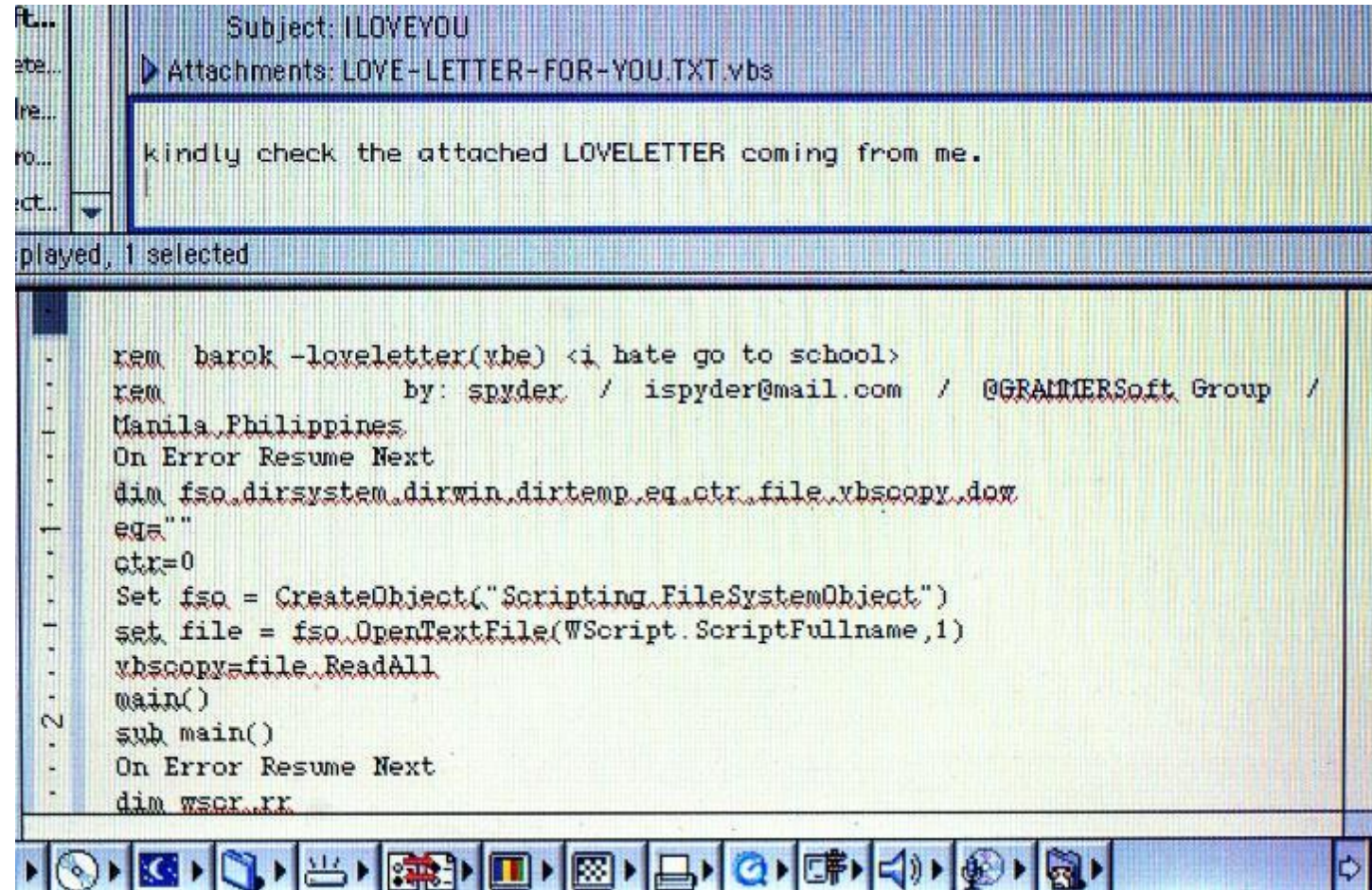
Important reference numbers: A5599796-2695577-

The price of 365 user applications is US\$189. The price of a lease for the lifetime of your hard disk is US\$378. You must enclose a bankers draft, cashier's check or international money order payable to PC CYBORG CORPORATION for the full amount of \$189 or \$378 with your order. Include your name, company, address, city, state, country, zip or postal code. Mail your order to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

Press ENTER to continue

ILOVEYOU worm

- Email worm
- Infected >50M users
- \$5.5B damage
- Spread as VBS script
- 2000 Overwrote random files
- Created by 24-year-old in Philippines
- Not covered by laws at the time



The screenshot shows an email client interface. The subject line is "Subject: ILOVEYOU". The attachment list shows "Attachments: LOVE-LETTER-FOR-YOU.TXT.vbs". The email body contains the text "kindly check the attached LOVELETTER coming from me." Below the email content, a VBS script is displayed in a code editor window. The script is as follows:

```
rem barok -loveletter(vbe) <i hate go to school>
rem          by: spyder / ispyder@mail.com / @GRAMMERSoft Group /
Manila,Philippines
On Error Resume Next
dim fso,directory,dirwin,dirtemp,eq,ctr,file,vbscopy,dow
eq=""
ctr=0
Set fso = CreateObject("Scripting.FileSystemObject")
set file = fso.OpenTextFile(WScript.ScriptFullName,1)
vbscopy=file.ReadAll
@main()
sub main()
On Error Resume Next
dim wscr,rr
```

Stuxnet

2010

- Targeted SCADA systems
- Damaged nuclear program in Iran
- Nation state attack
- Caused centrifuges to vibrate apart
- Infected >200,000 systems
- Spread with USB drives on an air-gapped system



Operational Technology Attacks

- Triton (2017): Targeted safety instrumented systems
- Ukrainian power grid (2015-2016): Malware caused loss of access and blackouts
- NotPetya (2017): Update from tax software destroyed data on OT systems
- Maroochy Shire (2000): Australian hack spilled millions of liters of sewage into parks and rivers
- Colonial pipeline (2021): Shut down oil flow for several days
- JBS (2021): Ransomware attack on meat processor disrupted supply chains
- Oldsmar water treatment (2021): Attacker increased lye content in water to dangerous levels
- SolarWinds (2020): Attackers inserted into Orion update, infecting 18,000 organizations

“I think from a software engineering perspective, it’s probably fair to say that [SolarWinds] is the largest and most sophisticated attack the world has ever seen”

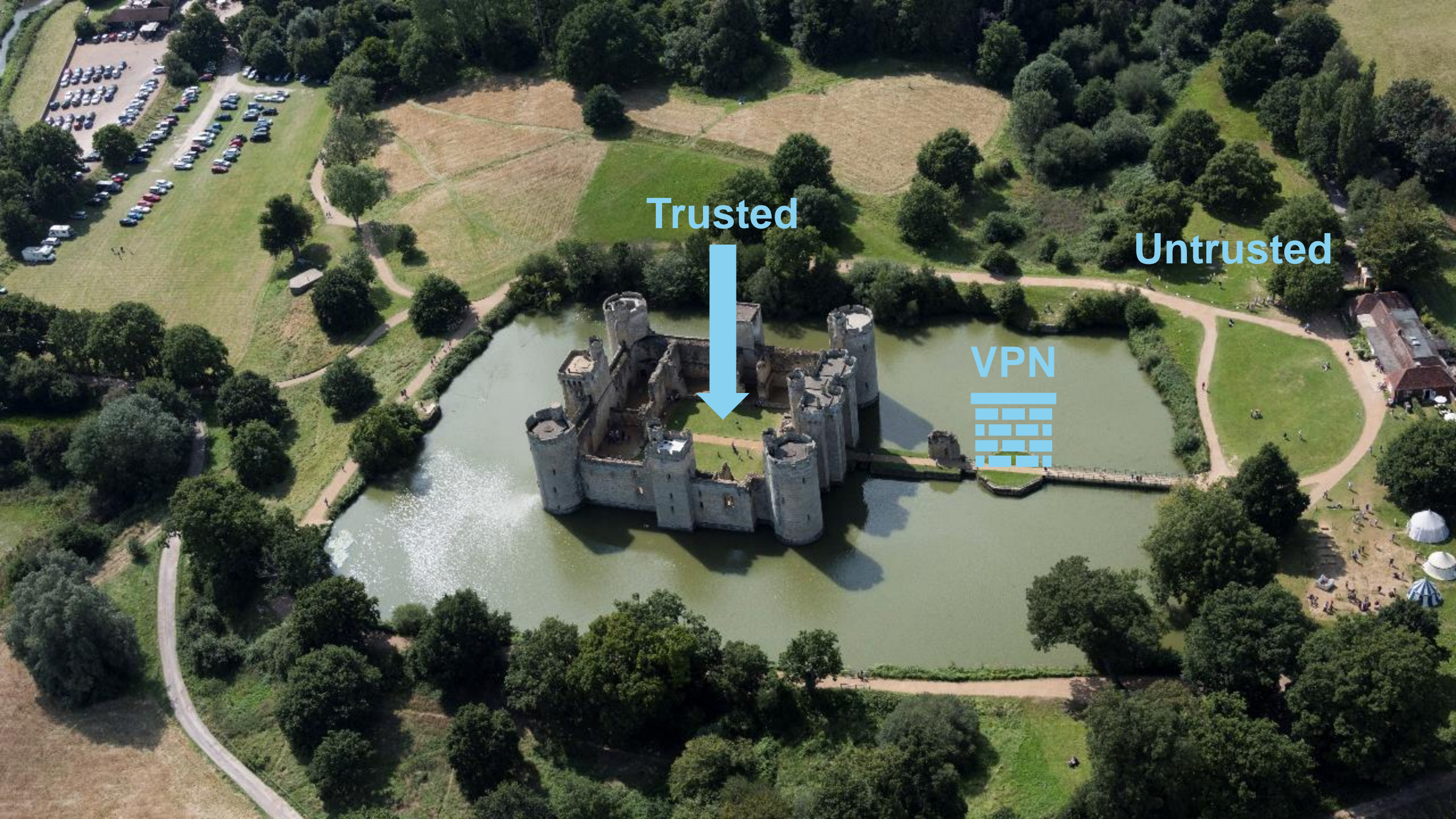
Brad Smith
President, Microsoft



“...we asked ourselves how many engineers have probably worked on these attacks. And the answer we came to was, well, certainly more than 1,000”

Brad Smith
President, Microsoft



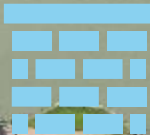


Trusted

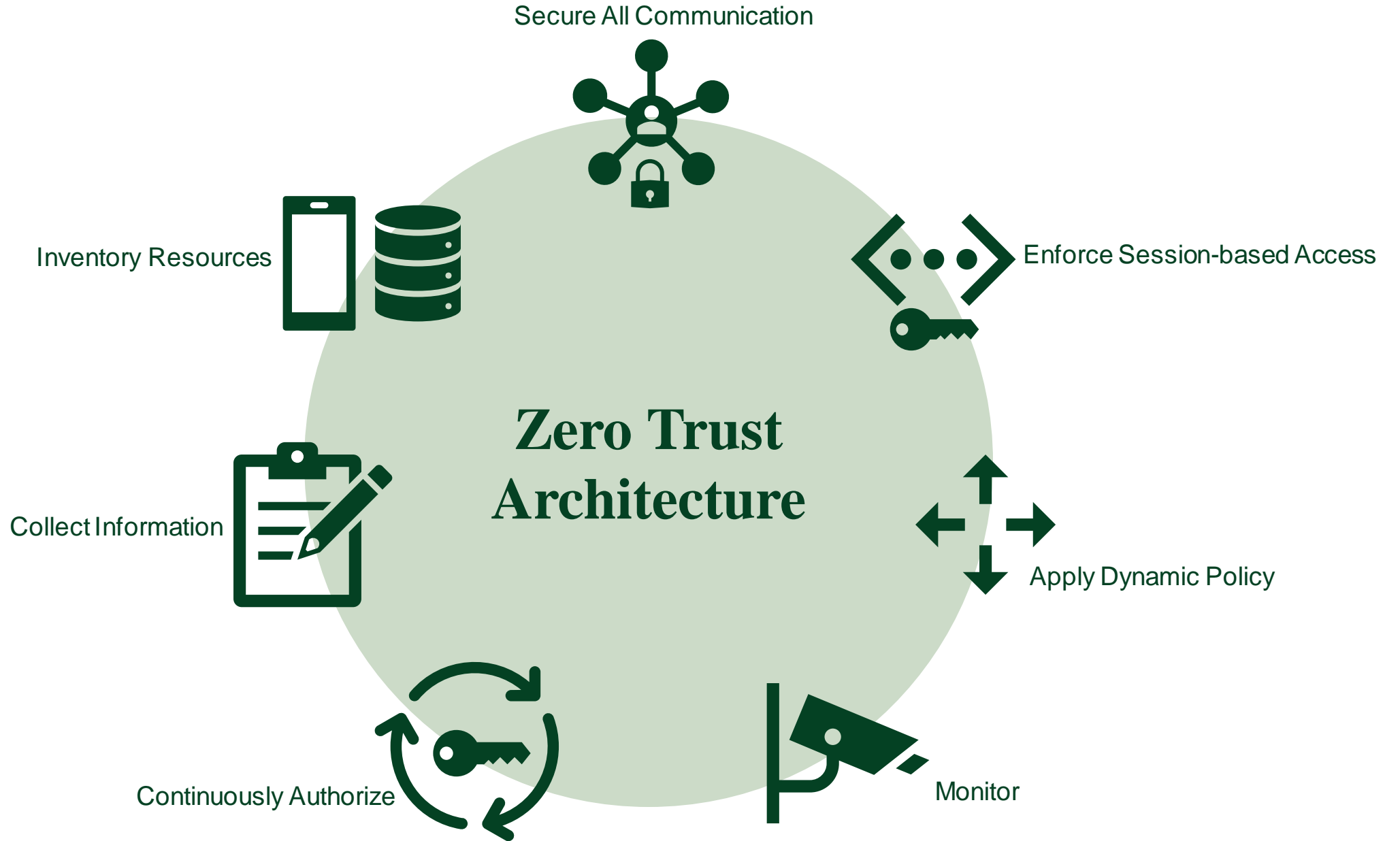


Untrusted

VPN







Zero Trust Example – Airport Security

Ticket Counter



Authenticate (ID)
Authorize (Ticket)
X-ray Bags

Security Checkpoint



Authenticate (ID)
Authorize (Ticket)
X-ray Person & Bags

Baggage Handling



Controlled Access

Gate



Access (Ticket)

Cockpit



Controlled Access

Pilot



Access (ID)

Secure All Communication



Inventory Resources



Enforce Session-based Access



Translation: Zero Trust Architecture

Your IT department does not trust your test system.

Collect Information



Apply Dynamic Policy



Continuously Authorize



Monitor



Your IT Team doesn't trust
your test system.



Your customer doesn't trust
your IT team.



The government doesn't trust your customer.





MAY 12, 2021

Executive Order on Improving the Nation's Cybersecurity



BRIEFING ROOM

The scope of protection and security must include systems that process data (information technology (IT)) and those that run the vital machinery that ensures our safety (operational technology (OT)).

sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy.

The Federal Government will continue to work with the private sector to protect against, and respond to, malicious cyber threats.

(ii) develop a plan to implement Zero Trust Architecture,

cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The

Government Controls on Secure Systems

- 1) Systems must receive authority to operate (ATO) before connection to the Federal network
- 2) Federal contracts for systems delivered by contractors must meet cybersecurity requirements
- 3) Customers with Federal contracts must protect contract data

These terms are enforced with the *Defense Federal Acquisition Regulation Supplement* – a list of terms passed from the government to suppliers through contracts.

RMF Process – Path to ATO

Risk Management Framework

- Required for all Federal agencies since 2014 under the Federal Information Security Modernization Act
- RMF process defined in NIST SP 800-37 document
- Requires that all systems connecting to the network be analyzed against NIST SP 800-53





DFARS Terms

DFARS 252.204-7012/7019/7020/7021

- Requires that any supplier assert that the data handling system meets NIST SP 800-171 requirements
- Adapted to operational technology with NIST SP 800-82





NIST Special Publications

NIST SP 800-171

- 110 Controls
- Applies to any system handling government contract information
- Applied to suppliers through DFARS contracts
- Basis for CMMC certification
- Applies to test systems used to produce systems for the government

NIST SP 800-53

- 1,600 Controls
- Applies to any system connecting to the Federal network
- Applied to agencies through FISMA
- Applied to suppliers by contract obligations for documentation
- Applies to test systems delivered to the government



Typical Requirements for test systems



- ❑ Restrict user access with unique passwords
- ❑ Run systems with least privilege access accounts
- ❑ Provide audit logs of user activity, data transfers
- ❑ Use only components with active support available
- ❑ Scan for viruses and malware
- ❑ Provide training to users on basic security hygiene
- ❑ Establish a baseline configuration
- ❑ Use multifactor authentication for local and network access
- ❑ Sanitize or destroy media before disposal or repair
- ❑ Prohibit use of storage devices with no identifiable owner
- ❑ Limit physical access to system



SECIMATION

Embedded Cybersecurity Challenges

Hal Aldridge, Ph.D., CEO
hal.aldrige@secmation.com
www.secimation.com

Background

Secmation is a small business located Raleigh, NC, specializing in Cybersecurity R&D and Product Development for applications including unmanned and autonomous systems.



Dr. Hal Aldridge is Founder/CEO of Secmation. Prior to founding Secmation, Dr. Aldridge served as CTO at Sypris Electronics, an information security company specializing in high assurance electronics and software used to protect sensitive communications and critical infrastructure. Before entering the cybersecurity industry, Dr. Aldridge developed robotic systems for NASA and Northrop Grumman. He holds a Ph.D. in Electrical and Computer Engineering from Carnegie Mellon University.

Modern Embedded and Test Systems

Modern embedded and test systems have possible security concerns

- Can be composed of hardware and software from multiple vendors. Do you really know what is in your system?
- What parts of your system are secure? How do you know they are? Can you prove it?
- Is your system “air gapped”? Do you have all the controls in place to make sure it ALWAYS stays that way? Not as easy as you think...
- What is your system connected to now? What will it be connected to tomorrow?
- How is the software updated? Are you using the same Windows 7 OS for the last decade? It works, right? Ready for Windows 11?
- And more.... They pay security people (physical or cyber) to be paranoid 😏

Cybersecurity requirements on embedded systems AND the systems that test them, previously minimal or non-existent, are becoming mandatory and evolving rapidly



Example: Modern Car Vulnerabilities

DARKReading The Edge DR Tech Sections ↕ Events ↕

ICS/OT Security | 5 MIN READ | NEWS

From Ferrari to Ford, Cybersecurity Bugs Plague Automotive Safety

Security vulnerabilities plague automakers, and as vehicles become more connected, a more proactive stance on cybersecurity will be required — alongside regulations.

 **Nathan Eddy**
Contributing Writer, Dark Reading

January 06, 2023



Source: Christopher Vincenti via Alamy Stock Photo

- A quick Google search brings up the current state of automotive cybersecurity. Not ideal, but better than a few years ago.
- Example of known vulnerabilities from <https://samcurry.net/web-hackers-vs-the-auto-industry/>
- Hyundai/Genesis
 - Fully remote lock, unlock, engine start, engine stop, precision locate, flash headlights, and honk vehicles using only the victim email address
 - Fully remote account takeover and PII disclosure via victim email address (name, phone number, email address, physical address)
 - Ability to lock users out of remotely managing their vehicle, change ownership

Cybersecurity and Safety

- NIST 800-53.... NIST 800-171... FIPS 140-3.... ISO/IEC 27001... Risk Management Framework... Authority to Operate...
- Like all industries, Cybersecurity has its own buzzwords and standards.
- ***Cybersecurity shares many of the same challenges as safety.*** The language can be confusing, the requirements unclear, and the rules not obvious.
- Like Safety, Cybersecurity is about risk. What is the likelihood of an event occurring? What are the consequences of an event if it occurs?
- Safety systems that depend on software ARE NOT SAFE if they are not secure.
- Full compliance to complex standards is hard.... But making progress in implementing cybersecurity protections that will significantly lower your risks can be much easier....

Case Study – Secure Industrial Control

- Secmation developed the Secure Communications module for the Navy Facilities Command (NAVFAC) to securely connect their Industrial Control System (ICS) equipment to Navy networks
- Information had to cross back and forth from Non-secure ICS networks to highly secure Navy IT networks
- Sound like a familiar challenge?
- How did we do it?



How Were We Successful

- IT is not OT.... OT is not IT.... Both have different cybersecurity needs and solutions to meet their specific needs. Know the difference. We implemented OT protocols for Modbus and others and translated them to IT protocols for transit. ***The traditional IT solutions for cybersecurity were not compatible with OT protocols, timing, etc.***
- Like all testing, understand the requirements BEFORE you design the test. Otherwise you can test for the wrong thing, miss a requirement, test for a requirement that is not applicable, etc. Like ANY other standard. We selected NIST 800-53 controls with customer for RMF testing and certified the equipment to FIPS 140-2. ***A very significant part of the total development effort was defining, getting ready for and performing testing. We knew what we were doing. Don't underestimate it.***
- Cybersecurity is no longer optional. It is becoming a requirement for almost any computer system doing something important OR that could provide an attacker access to an important system. No such thing as an “air gap”. ***The customer needed this solution because they needed to connect air-gapped systems that were not designed to be connected.***

For more information contact: Hal Aldridge hal.aldridge@secmation.com

These may translate to you as:

- Requests for documentation:
 - Bill of material / Software bill of materials
 - Letters of volatility
 - Compliance documents to 800-171 / 800-53
 - STIGs
- Requests for certification
 - FedRAMP for cloud services
 - ICD-503 software security
- Security testing
 - Static code analysis
 - Dynamic system analysis
 - Vulnerability scans
 - Penetration testing





NI Resources for security

ni.com/security – first stop for security information



Security

At National Instruments, we view the security of our products as an important part of our commitment to our customers. Use this page to stay informed and act upon security alerts and issues.

Subscribe to Security Announcements

We distribute security information through our Security-Announce mailing list. You can subscribe via our communications preferences page and opt out at any time.

We may provide additional information through the NI Update Service, Security Updates page, customer-provided contact information, and the US National Vulnerability Database.

[Subscribe to Security Announcements](#)

Download Security Updates

The NI Update Service is the primary mechanism for distributing security updates for installed software. Security and other critical updates are also listed and available for download on the Security Updates page.

[Download Security Updates](#)

Report a Security Issue

We encourage you to report security vulnerabilities to us privately so that we can follow a coordinated disclosure process, allowing us time to thoroughly investigate security issues and publicly disclose them when appropriate.

To report security issues in our products or on ni.com, email security@ni.com with sufficient details about how to reproduce the issue. You may use the [NI PGP key](#) to encrypt any sensitive communications you send to us. When you notify us of a potential security issue, our remediation process includes acknowledging receipt and coordinating any necessary response activities with you.

For all other support issues, use one of our [technical support contact methods](#).



NI Resources for security

ni.com/security – first stop for security information

security@ni.com – report issues, request information

Letters of volatility – with product manuals or at ni.com/letters-of-volatility

Secure development guides – at ni.com/security

Additional security documentation – available on request



Security

At National Instruments, we view the security of our products as an important part of our commitment to our customers. Use this page to stay informed and act upon security alerts and issues.

Subscribe to Security Announcements

We distribute security information through our Security-Announce mailing list. You can subscribe via our communications preferences page.

We may provide additional information through the NI Update Service, Security Updates page, customer-provided contact information, and the NI Product Database.

[Subscribe to Security Announcements](#)

Download Security Updates

The NI Update Service is the primary mechanism for distributing security updates for installed software. Security and other critical updates are available for download on the Security Updates page.

[Download Security Updates](#)

Report a Security Issue

We encourage you to report security vulnerabilities to us privately so that we can follow a coordinated disclosure process, allowing us to address security issues and publicly disclose them when appropriate.

To report security issues in our products or on ni.com, email security@ni.com with sufficient details about how to reproduce the issue. You should encrypt any sensitive communications you send to us. When you notify us of a potential security issue, our remediation process includes coordinating any necessary response activities with you.

For all other support issues, use one of our [technical support contact methods](#).

NI Test System Security Summit

Semi-annual meeting for test engineers, security teams, and IT professionals

Online forum to access discussions, presentations

Next meeting: October 2023

To be invited:

Email steve.summers@ni.com





NI Investments in Security

Product
security
documentation

Product
STIGs

FedRAMP
certification

Secure
development
guides

Secure development process

CMMC certification

More Information

security@ni.com

ni.com/security

steve.summers@ni.com

