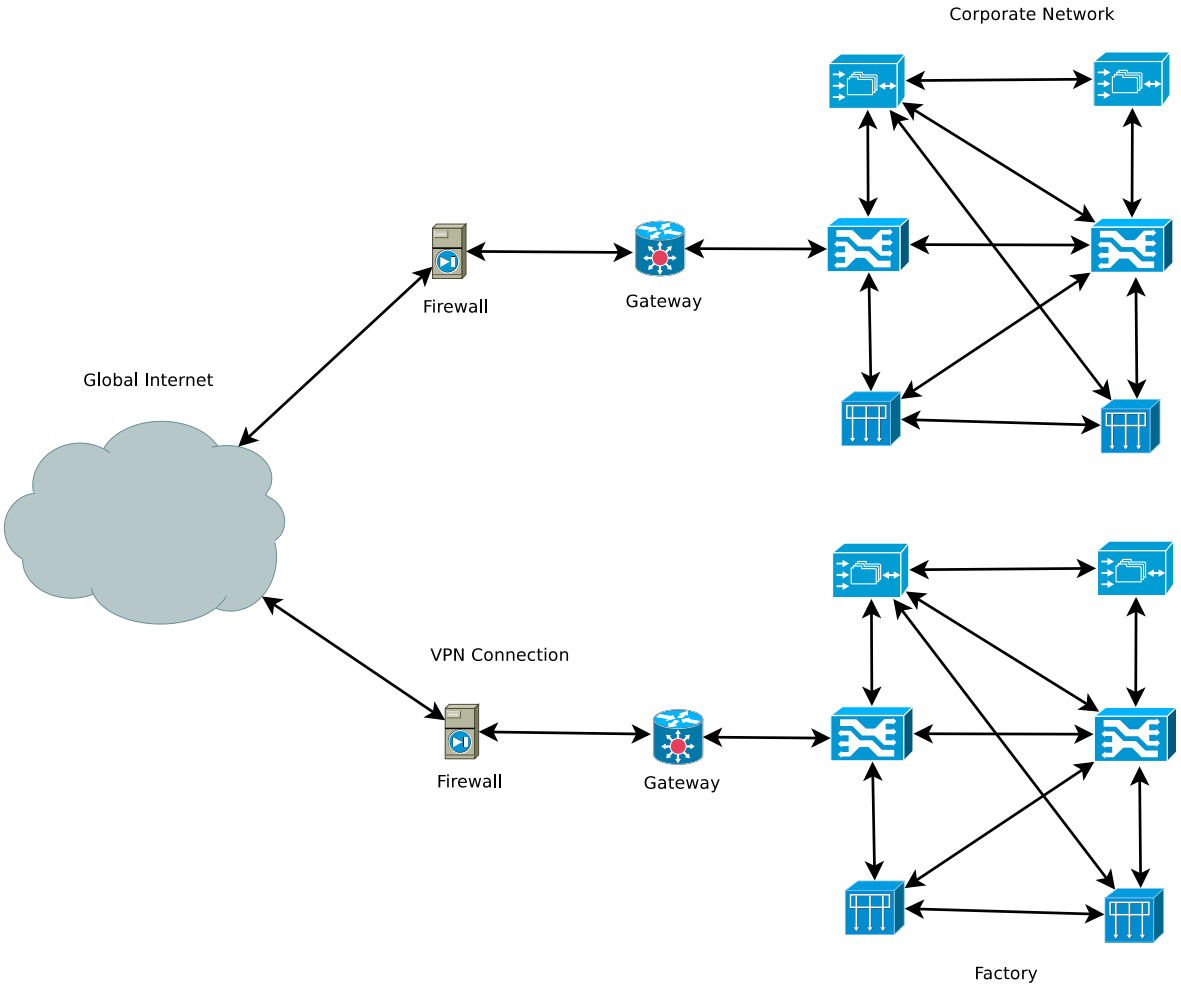
Evolution of the Attack Surface

R. R. Brooks – rrb@acm.org
Clemson University, Electrical and Computer Engineering

July, 2019

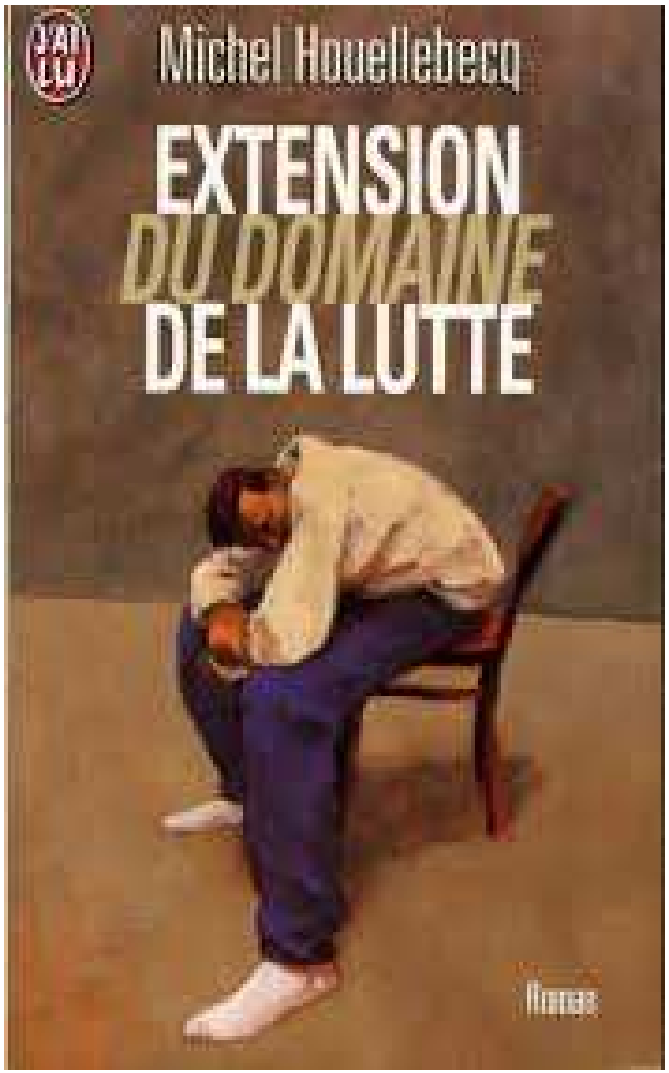
Traditional Security



Attack Surface

- Network firewalls block questionable access.
- Communications pass through manageable gateways.
- Outward facing interfaces are limited.
- Incoming connections/interfaces are armored.
- Meant to limit attacker access to the system.
- Ports of entry will be fortified.

Larger Battlefield



Attack Surface is Fiction

- Why?

Attack Surface is Fiction

- Why?
- Because you do not control which machines connect to your network.

Attack Surface is Fiction

- Why?
- Because you do not control which machines connect to your network.
- Because your hardware vendors do not control what is in their products.

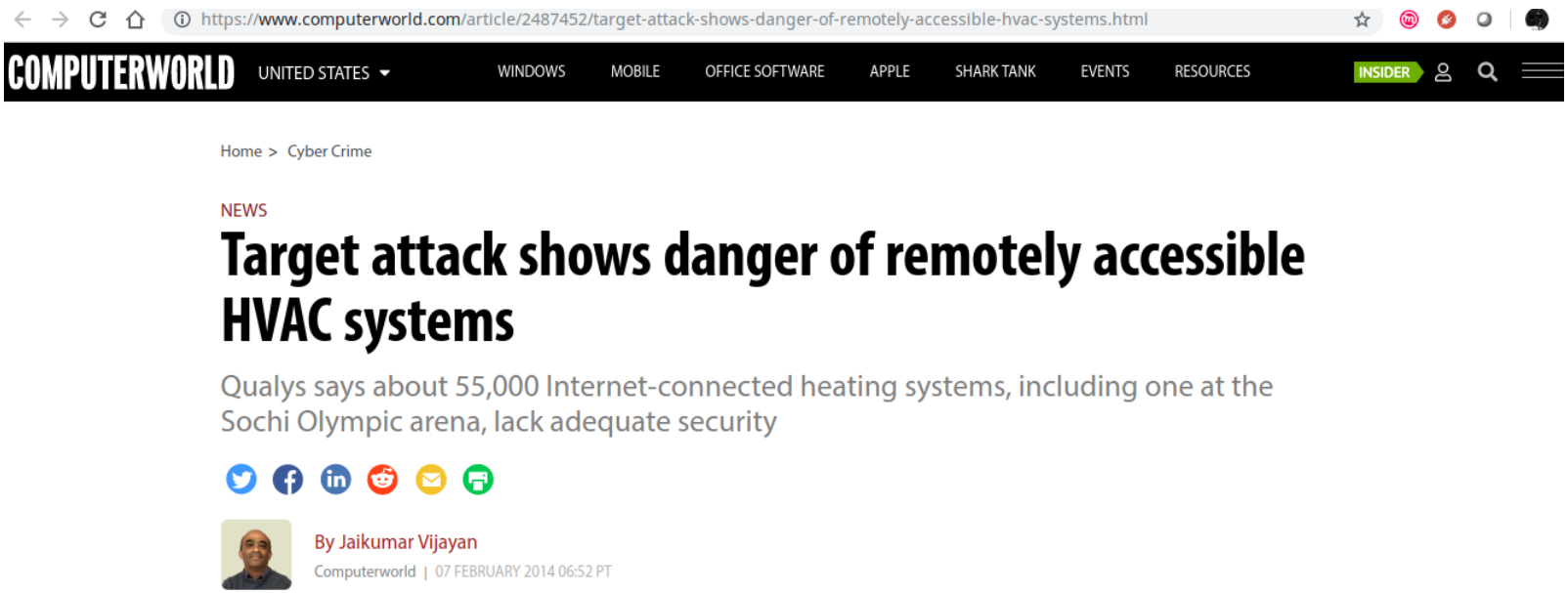
Attack Surface is Fiction

- Why?
- Because you do not control which machines connect to your network.
- Because your hardware vendors do not control what is in their products.
- Because your software vendors do not control what is in their products.

Attack Surface is Fiction

- Why?
- Because you do not control which machines connect to your network.
- Because your hardware vendors do not control what is in their products.
- Because your software vendors do not control what is in their products.
- Because no one controls Internet routing.

Supporting Infrastructure



https://www.computerworld.com/article/2487452/target-attack-shows-danger-of-remotely-accessible-hvac-systems.html

COMPUTERWORLD UNITED STATES WINDOWS MOBILE OFFICE SOFTWARE APPLE SHARK TANK EVENTS RESOURCES INSIDER

Home > Cyber Crime

NEWS

Target attack shows danger of remotely accessible HVAC systems

Qualys says about 55,000 Internet-connected heating systems, including one at the Sochi Olympic arena, lack adequate security

By Jaikumar Vijayan

Computerworld | 07 FEBRUARY 2014 06:52 PT

Target Breach

- In Dec 2013, Target data breach exposed.
- 40 million credit cards and PII of 70 million people.
- Target settlement cost $18.5 million.
- Malware stole credentials from HVAC vendor.
- HVAC vendor interfaced with Target for electronic billing and project management.
- Once in network attackers maneuvered to POS devices.
- Estimated >= 55,000 HVAC vendors have access to companies for remote monitoring of energy, etc.
- BACNet systems: elevators, security, smart grid, power meters, etc.

Bring your own device – BYOD

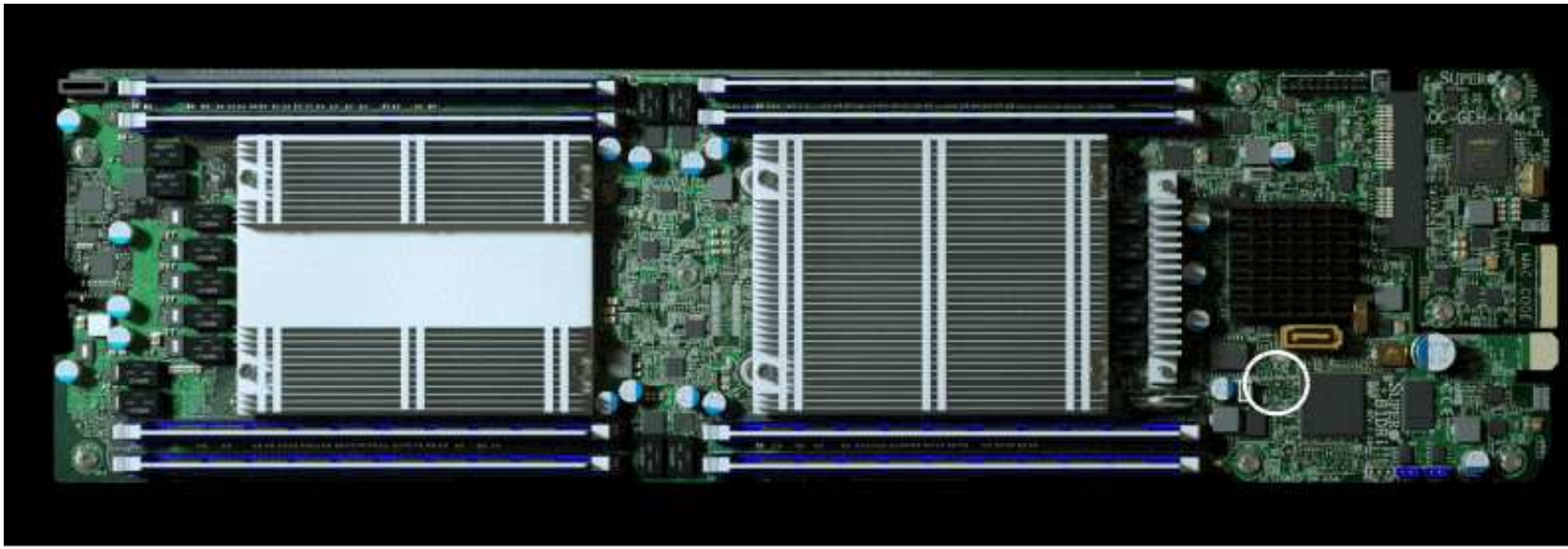
- Employee devices behind firewall, on wireless, etc.
- Companies enforced BYOD policies, but stopped.
- Too many devices, operating systems, and apps.
- Unsafe behavior of employees outside of work.
- Too expensive and employees not cooperating.
- Banning mobile devices results in geriatric work force.

Who is on your network?

- HVAC, power, security, elevator, all IoT.
- Tried to buy a non-smart TV lately?
- All employee devices.
- Poorly secured consumer devices.
- Device designs help vendors spy on customers.
- IoT devices not designed for security.
- Device security maintained by non-experts.
- Not to mention cloud based out-sourcing.
- You lost control years ago.

Hardware Implant

Can you see it?



Hardware implant 1

- Bloomberg reports hardware implants in AWS servers.
- Claims implants Chinese backdoors to servers.
- Bloomberg story controversial.
- Amazon denies. US Intel sources confirm.
- No one claims **impossible** or *unlikely*.
- Hardware supply chains pass through multiple companies/countries.
- Implants hard to detect with quality control.

Hardware implant 2

- Snowden – NSA implants inserted during shipment.
- Suspected hardware kill switch stopped Syrian radar when Israel attacked Dayr al-Zawr facility.
- Suspected French remote ability to stop advanced capabilities in military hardware.
- Detection of hardware Trojans unsolved research problem.
- Made worse by outsourcing of production.
- Nano-scale Trojans possible.
- Nano-Trojan detection would require electron microscope.

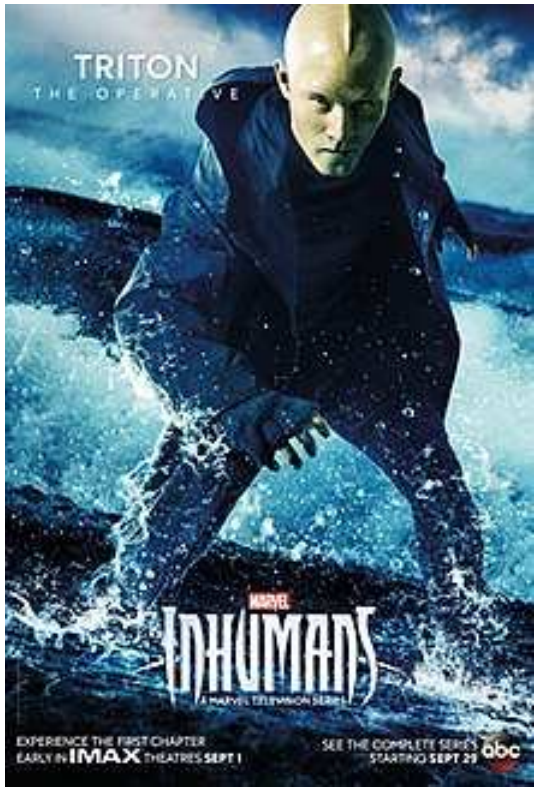
01_May_2008_The_Hunt_for_the_Kill_Switch_IEEE_Spectrum

Hard Disk Malware

- Hard disk drive (HDD) firmware malware.
- Invisible and almost indestructible.
- Equation cyber-espionage group.
- "Rare as pandas walking across the street"

www.kaspersky.com/blog/equation-hdd-malware/7623/

Triton



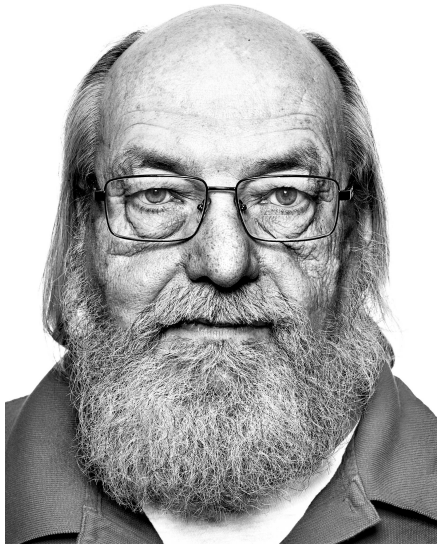
- Triton industrial control system malware.
- Inserts malware into safety control system logic.
- Meant for high impact damage to industrial control.

www.antiy.net/p/antiy-released-technical-analysis-of-industrial-control-malware-trisis

Hardware conclusions

- Hardware attacks rare for now.
- Known attacks mainly by nation states.
- Industry vulnerable as critical infrastructure.
- Nation state attacks leak the technology to less sophisticated attackers.
- Lower level attackers re-use the technology.
- Kaspersky sells UEFI (hardware root of trust) anti-virus.
- Existence of hardware root of trust anti-virus market is worrisome.
- Hardware is mainly firmware (software).
- Hardware is not inherently more secure.
- Replacing hardware costs money, so hardware vendors test.

On Trusting Trust



- Nice to be able to fix Unix systems.
- Insert backdoor into login.
- Remove login backdoor insert into C compiler.
- Compiler inserts login backdoor.
- Use compiler to compile C compiler with clean source.
- Able to insert malware with nothing bad in source code.

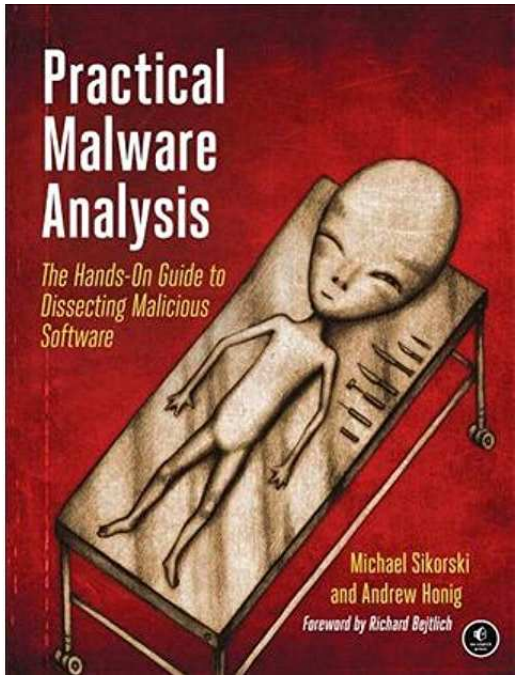
CCleaner and ASUS

- Stolen TeamViewer credentials used to infect Crap Cleaner, which was used to infect 40 companies with ShadowPad.
- ASUS ShadowHammer update pushed signed infected updates to BIOS and UEFI.
- Up to 1,000,000 ASUS machines infected, concentrated on 600 specific machines identified by MAC address.
- ShadowHammer linked to ShadowPad.

Supply Chain

- Security orthodoxy: **Keep patches up to date!**
- Really? Similar attacks:
  - NotPetya,
  - Havex(Industrial Control systems),
  - Juniper networks source code,
  - iOS fake developer tool,
  - Android,
  - Python,
  - Javascript.
- According to NIST: Supply chain attacks the *New Normal*.

Dynamic Libraries/Shared Objects

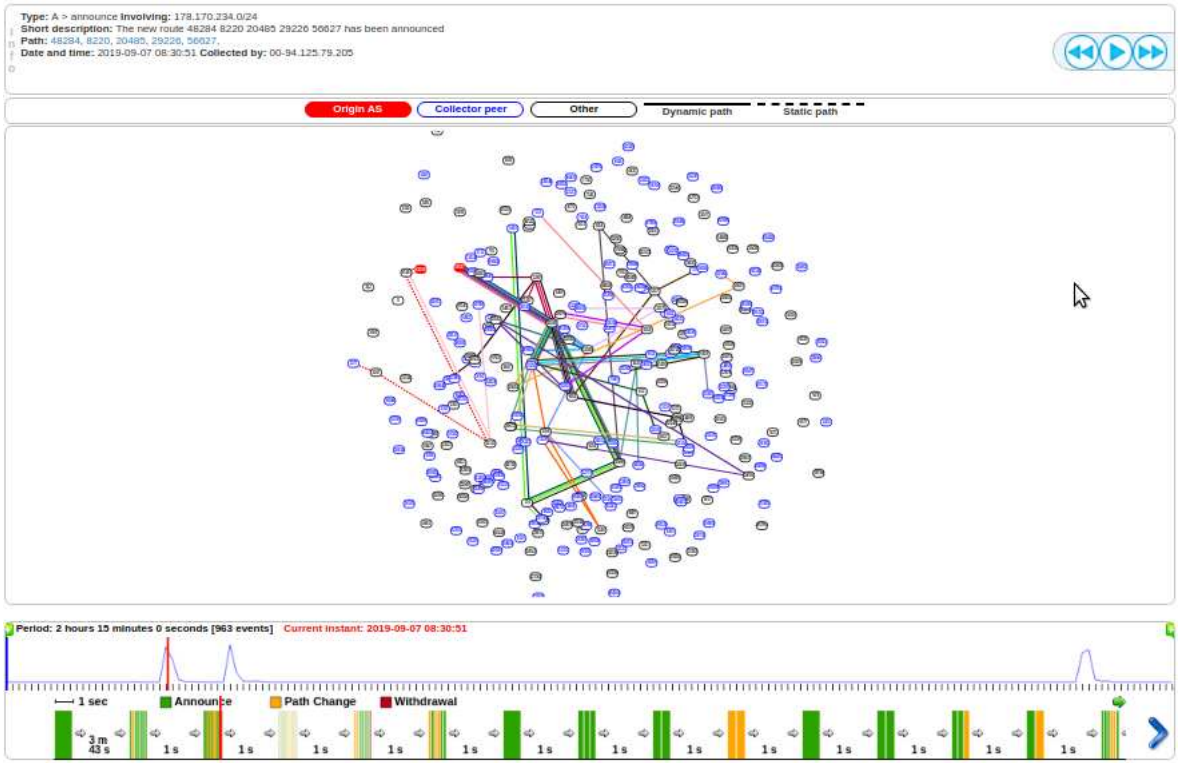


- Standard malware reversing text 2 DLL chapters.
- Chapter 11 – Malware behavior, DLL Hijacking.
- Chapter 12 – Covert malware launching, DLL injection.
- Standard way to insert malware into processes.

Network Routes Insecure

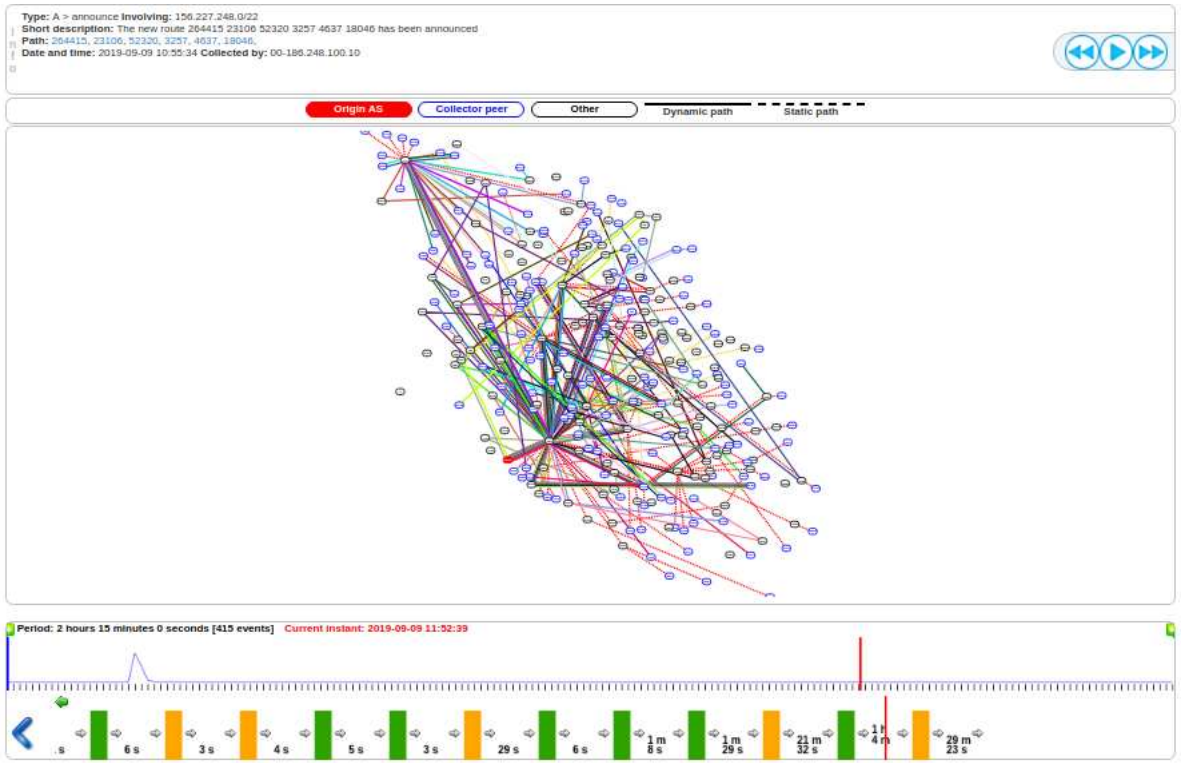
BGPStream.com

Network Routes Insecure-Russia



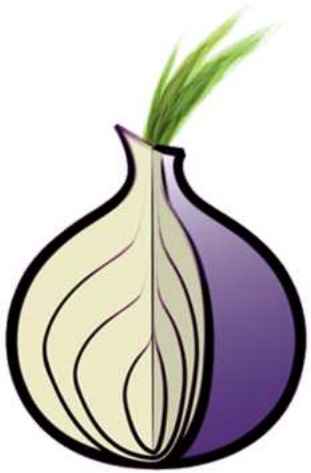
- Interdomain routing not secured.
- Denial of Service is trivial.
- Routing of traffic for surveillance is trivial.

Network Routes Insecure-Hong Kong



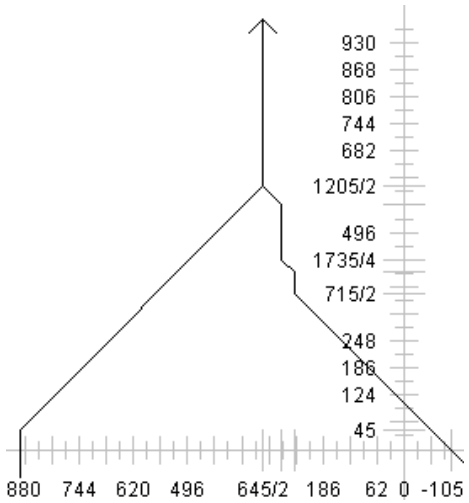
- China points of presence can hijack US traffic at will.
- Nigerian Google Traffic routed through China and Russia.
- Taiwan DNS traffic routed through Brazil.

Deterministic builds



- Tor software produces identical (linux) binary builds on any system.
- Allows local build from source, comparison to downloads.
- Resistance to supply chain attacks.
- Odd that we have to rely on crypto-anarchists for this.

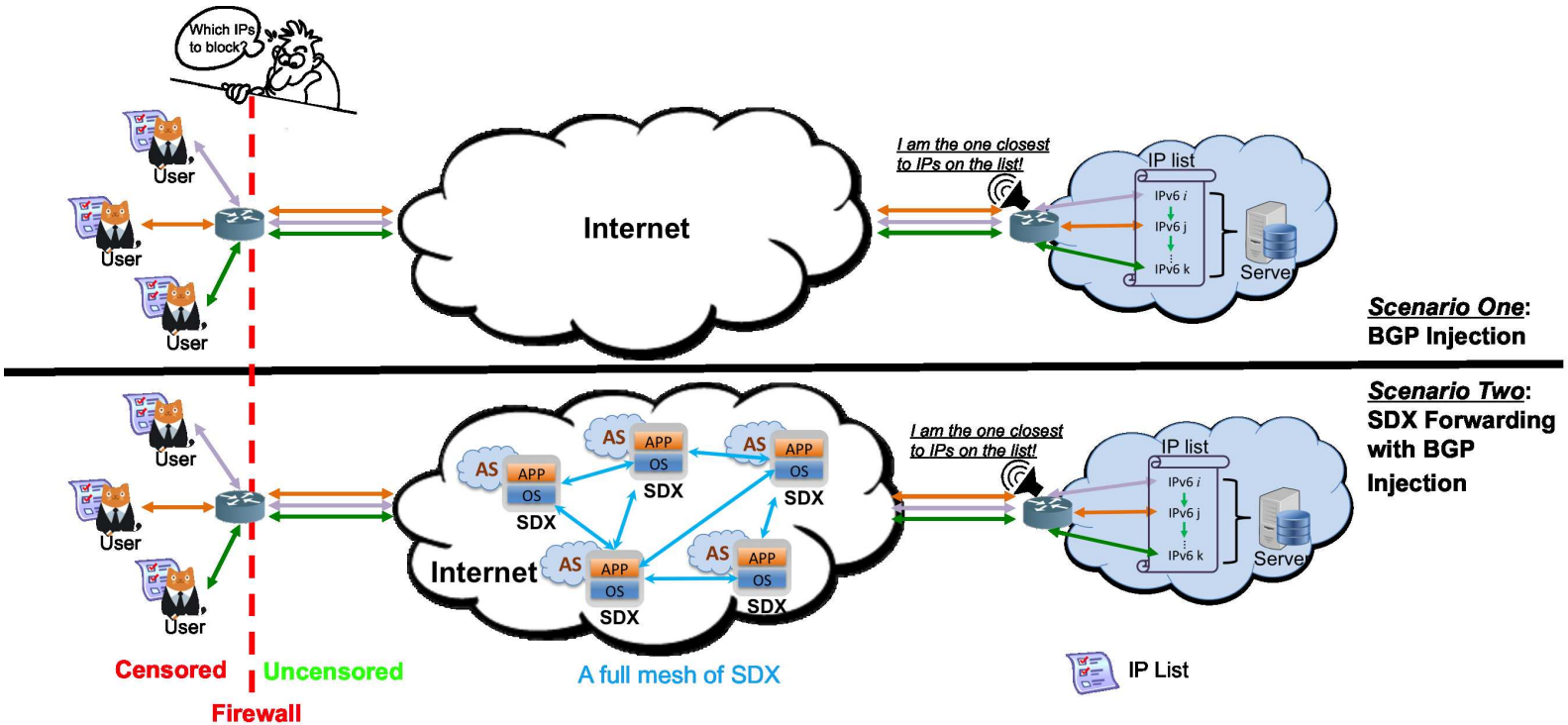
Combinatorial Game Theory



- Pardon my math.
- Game shown $== \{970|880||\{610|-105||-280|-840\},\{280|-840\}\}$
- We are now competing at many levels on many machines.
- Math to find best answer PSPACE complete, much worse than NP Complete.
- Finding answer within known constant offset of optimal is O(N).
- We can use math to prioritize responses.

Traffic Analysis Resistant Network (TARN)

- Alternative network architecture removes vulnerabilities exploited by a variety of attacks (DNS/IP filtering, DDoS attacks, MITM attacks, etc.) by disassociating the relationship between IP prefixes and destination.
- End-to-end communication sessions have dynamic, short-lived, pseudo-random IPv6 addresses drawn from a range of IP prefixes rather than one.
- BGP injection and cyber-squatting integrated into software-defined Internet exchange points (SDX).



Blockchain

- Cryptocurrency is 'Honestly Useless': Harvard Cryptographer – *Bruce Schneier*
- Economist Nouriel Roubini Says 'Blockchain Is Useless, All ICOs Are Scams'
- "Blockchain is not only crappy technology but a bad vision for the future" –Kai Stinchcombe
- "Bitcoin Is Ridiculous. Blockchain Is Dangerous" – Paul Ford
- "Blockchain is a useless technology" – Glenn Chan

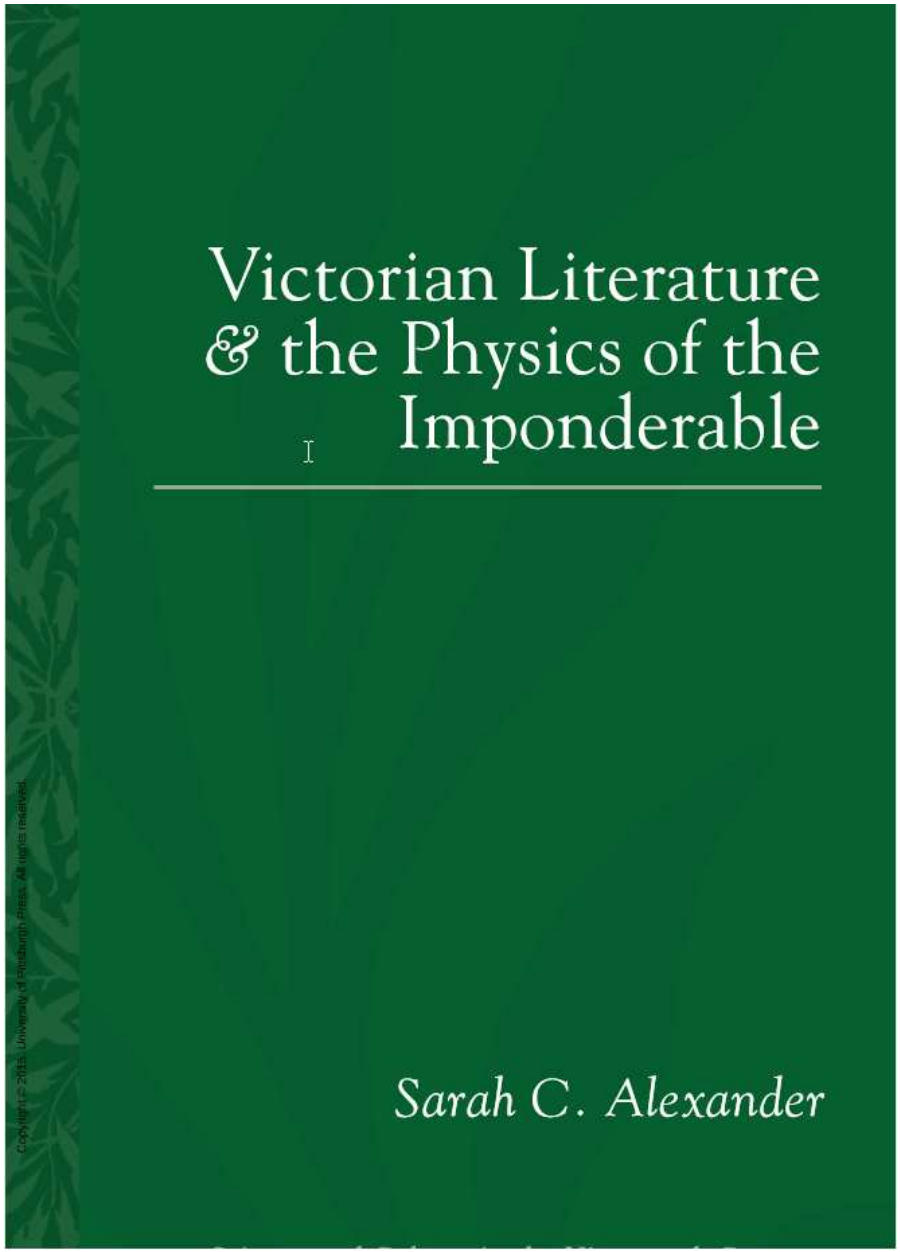
Smart contracts

- ☐ Secure distributed computation.
- ☐ Computation correctness guaranteed by parallel execution and BGP.
- ☐ Challenges:
  - Currently run in parallel on all nodes.
  - Currently dialect of **javascript** :(
  - Inputs restricted.

Summary

- Attack surface can no longer be limited:
  - Current electronics allow network access everywhere.
  - Hardware from vendors no longer secure.
  - Supply chain attacks make all software vulnerable.
  - Network paths can go anywhere.
- Possible solutions:
  - Deterministic builds against software supply chain.
  - Network traffic obfuscation.
  - Build strategic thinking into security tools.
  - Blockchain and smart contracts create security from distributed computers.

Questions?



O

https://www.jstor.org/stable/j.ctt1dwst10