Firewalling: Passwords, Financial Transactions and Human Privileges from CPU Resident Malware

Jim McAlear – Dec. 11, 2014

jim.mcalear@ieee.org

Smart-Phones for Two-Factor Authentication?

- Passwords, credit card numbers etc. neither safe for entry into smart-phones nor into PCs

- Will cost web retailers too much
  - already too much fall-off of customers during check-out phase of web-purchases (where’s my wallet?) – requiring another device makes things much worse (now where’s my phone – in the car?)

- Un-workable within enterprises – e.g. financial institutions
  - are IT groups going to support myriad of employee-owned devices – where are the phones – at home, in the car, in a meeting room, in a restaurant etc.? What happens when lost, stolen, damaged, disconnected, given to kids?
  - are IT groups going to purchase company smart-phones for employees – have them carry personal and business devices – where are they - are they fully charged etc.

Un-workable, costly band-aid, to underlying flawed design

Design Computers According to Asimov’s Law

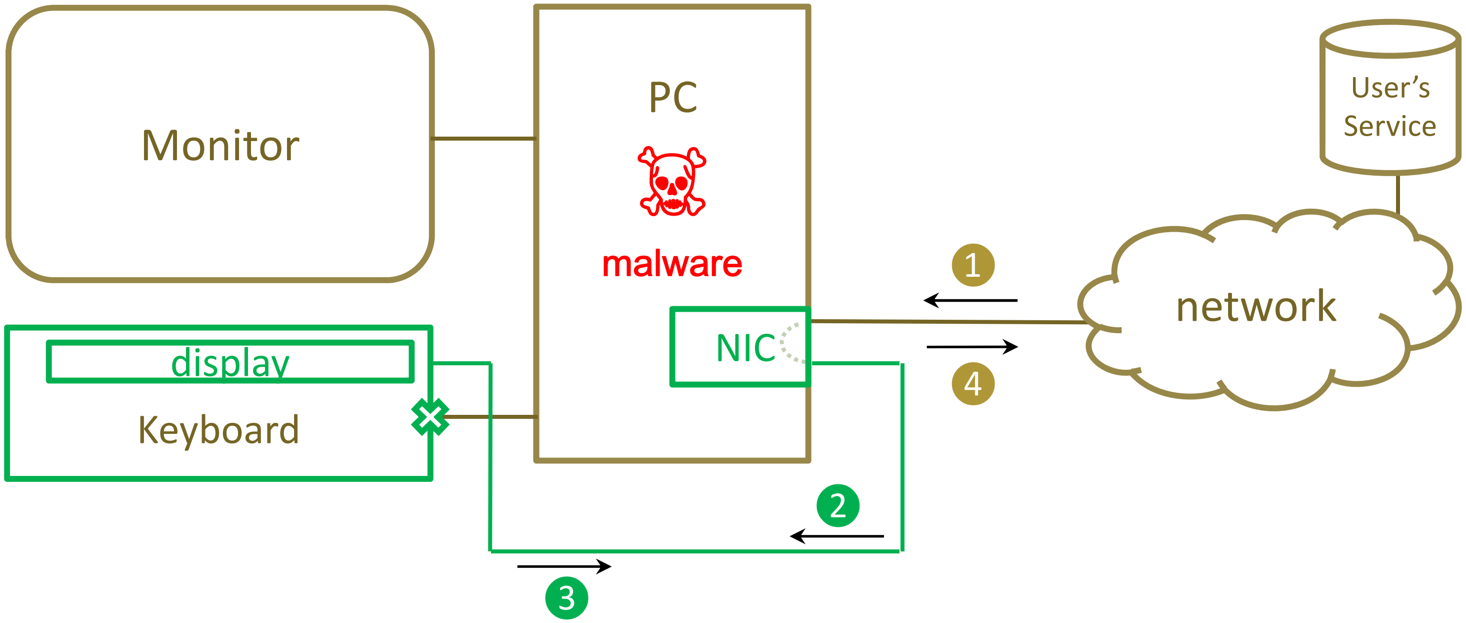
- ❑ Asimov’s Law privileges humans over smart machines
  - Law 1: robots must not harm humans (so neither should computers)

- ❑ People care strongly about Asimov’s Law
  - Elon Musk on Artificial Intelligence (AI): “summoning the demon”
  - Stephen Hawking on AI: “will destroy humanity”
  - ordinary users currently take Law into their own hands: will tape over camera lenses on laptops, will tape foam over microphones – as they assert ultimate privilege of determining what gets recorded or not in their environment – not the smart machine

Will reveal computer designs that adhere to Asimov’s Law
- smart machines will not be privileged to handle:
passwords, credit card numbers etc.

Protection of Credentials & Transactions

Credentials transactions bypass CPU and malware

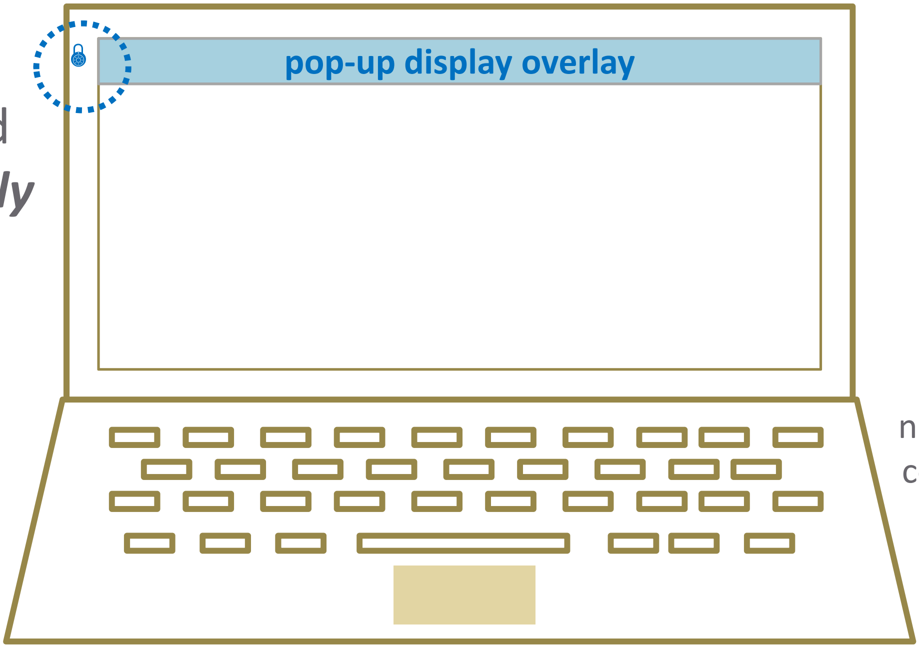


- New NIC functionality and connection redirects credentials request message (e.g. http 401 message) around CPU/malware to new display on keyboard
- Conventional keyboard connection is blocked until transaction is complete
- **No smart-machine/malware access to credentials**

Notebook / Tablet Internalized Solutions

Internalized configuration needs external lamp to indicate security mode operation

Pop-up display overlay and external lamp are ***exclusively*** under control of NIC



no room for LCD on compact keyboard

- Display overlays common on monitors – e.g. brightness/contrast controls
- Display overlays not accessible to OS – e.g. Print Screen can't capture
- For tablets, lamp indicates keyboard touch-input is disconnected from CPU

Humans Validate/Complete Transactions

🔒 [www.bank1.com] Transfer $128.64 to 8192-4096-2048 – enter PIN: <f1 - help>

🔒 [www.broker1.com] Purchase 400 shares of Telus Preferred – enter PIN: <f1 - help>

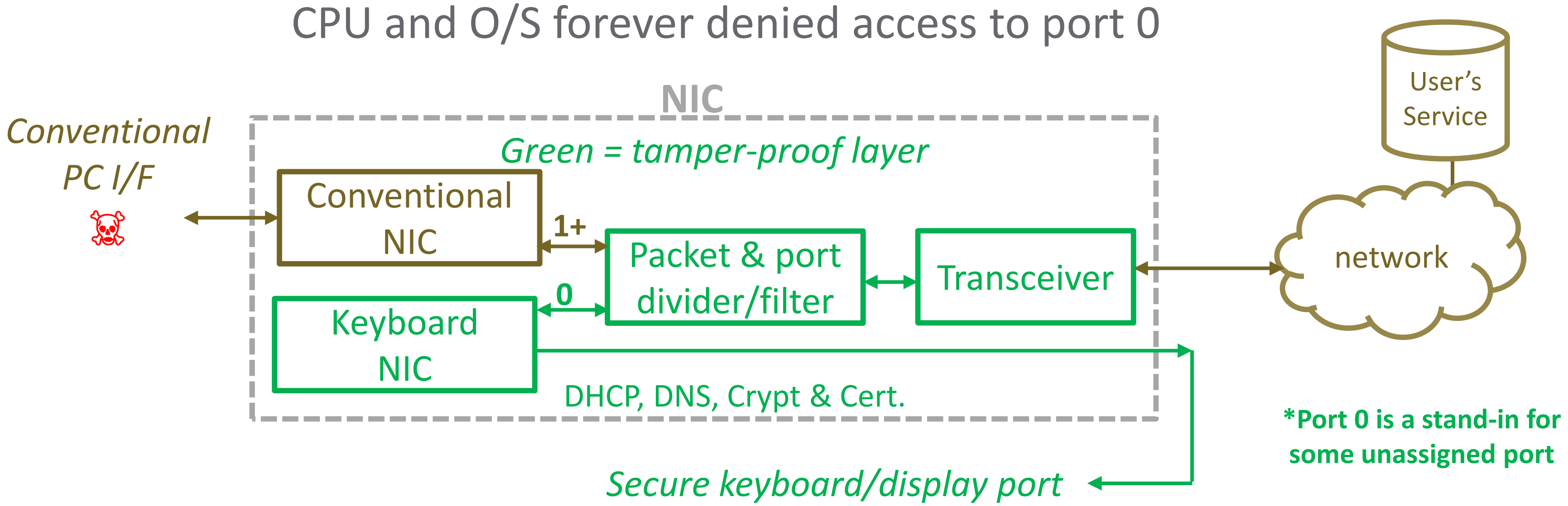
🔒 [chapters.indigo.ca] $64.16 purchase to 128 Byte St. – enter MasterCard: <f2 - more>

🔒 ????www.bankl.com???? Enter password: <?? f8 – warnings ??>

- Prevents smart-machine/malware from completing transactions
  - once user signs into bank/broker, require user to confirm risky transactions
  - especially needed for transfers to 3rd party accounts or stock purchases
  - not strictly necessary for modest transactions to well-established billers
- Prevents malware from tampering with purchase and shipping details
  - user alerted to unintended purchases and delivery elsewhere
- Memory for frequently used sites/certificates can alert to phishing

User Termination of Port 0* – Solves the Turing Test

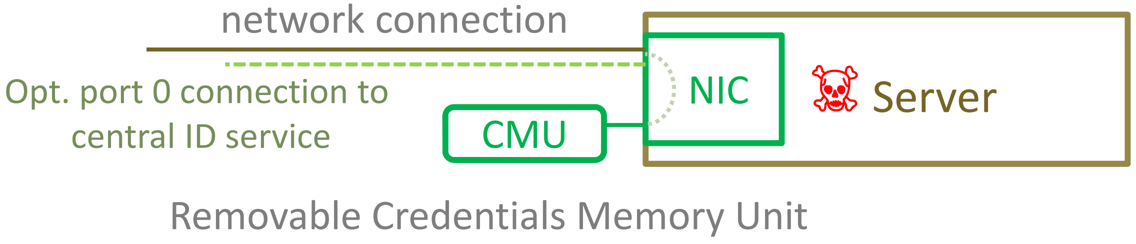
Port 0 dedicated to secure keyboard & display,
CPU and O/S forever denied access to port 0



*Port 0 is a stand-in for some unassigned port

- Placing service on separate Port 0, makes it general, aiding many services
  - akin to DNS Port 53: helper for HTTP, HTTPS, FTP, POP, SIP etc.
- NIC functions block malware from ever using UDP/TCP Port 0
- **Critical transactions involving Port 0 cannot be completed without human intervention and oversight!**
- Secure user-agent can have factory certificate from dedicated CA
  - allows server to confirm PC has secure hardware

Protection at Enterprise Server

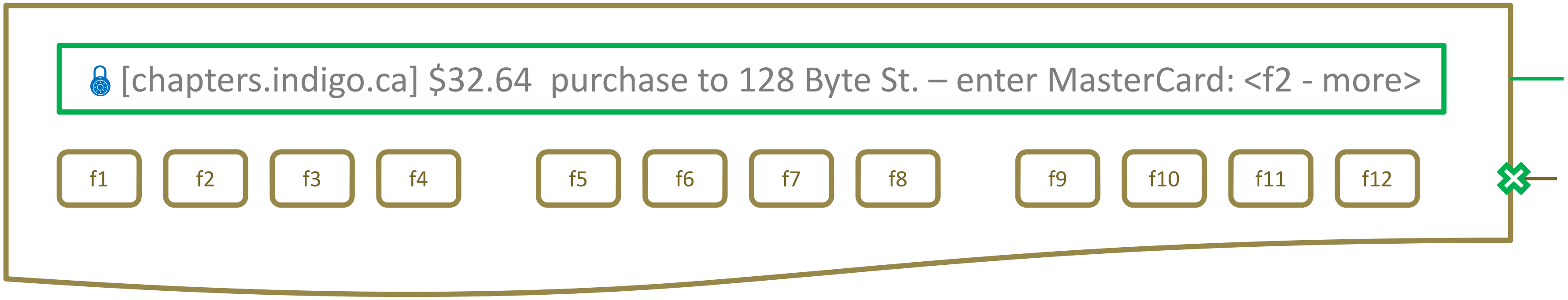

network connection
Opt. port 0 connection to central ID service
CMU
NIC
☠ Server
Removable Credentials Memory Unit

- Credentials not actioned within server – not accessible by CPU/malware
  - therefore cannot exploit services on other servers using valid credentials

- When server requires user authentication, it sends message to NIC to conduct transaction, and only receives a success/fail response
  - returned (http) authentication headers stripped by NIC – cannot reach CPU
  - could enhance CMU to clear credit-card transactions away from CPU

- Port 0 separation would allow connection to central ID service

What Does Success Look Like: It’s in Users’ Hands Worldwide & Users No Longer Helpless



🔒 [chapters.indigo.ca] $32.64 purchase to 128 Byte St. – enter MasterCard: <f2 - more>

- User can confirm web site name and/or welcome phrase, certificate
- Can verify transaction details & confidently submit credentials
- Provides two-factor authentication – conveniently within same device via independent means & “2nd factor” is fixed circuitry – not “smart”
- **Critical transactions just can’t complete without human oversight and explicit participation – only humans have this elevated privilege**
  - **CPU-OS can never complete a transaction – even if it were to know credentials!**

Fully compliant with Asimov’s design law

- smart machines never privileged to handle password, credit card etc.

Going Forward Plan

Formula for Insertion into Industry Ecosystem

❑ Involves a limited amount of funding

❑ Requires only a modest amount of readily available talent

❑ Has an inconsequential barrier to entry

❑ Has only modest technical challenge & few/quick steps

❑ Follows a proven & well-traveled road to success

Submission to Internet Engineering Task Force

Server-Side Adherence

Windows
Unix
Apache
Oracle-Java
Microsoft .Net
…

Networking Adherence

Huawei routers
Cisco VPNs
HP Firewalls
IBM SDN/VE
…

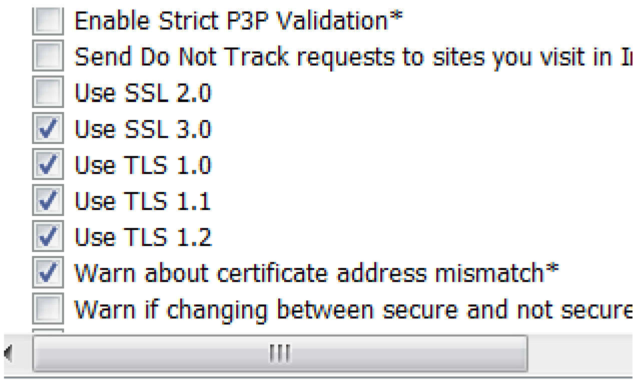
IETF Standards Activities

IPv4
IPv6
TCP
UDP
DNS
FTP
HTTP 1.0
HTTP 1.1
SSL 2.0
SSL 3.0
TLS 1.0
TLS 1.1
TLS 1.2
DTLS 1.2
…

Client-Side Adherence

Windows / IE
Unix / Firefox
Chrome OS / Chrome
Apple iOS / Safari
…

Screen shot of IE Options



☐ Enable Strict P3P Validation*
☐ Send Do Not Track requests to sites you visit in I
☐ Use SSL 2.0
☑ Use SSL 3.0
☑ Use TLS 1.0
☑ Use TLS 1.1
☑ Use TLS 1.2
☑ Warn about certificate address mismatch*
☐ Warn if changing between secure and not secure

Zero barrier to IETF participation – Universities very common

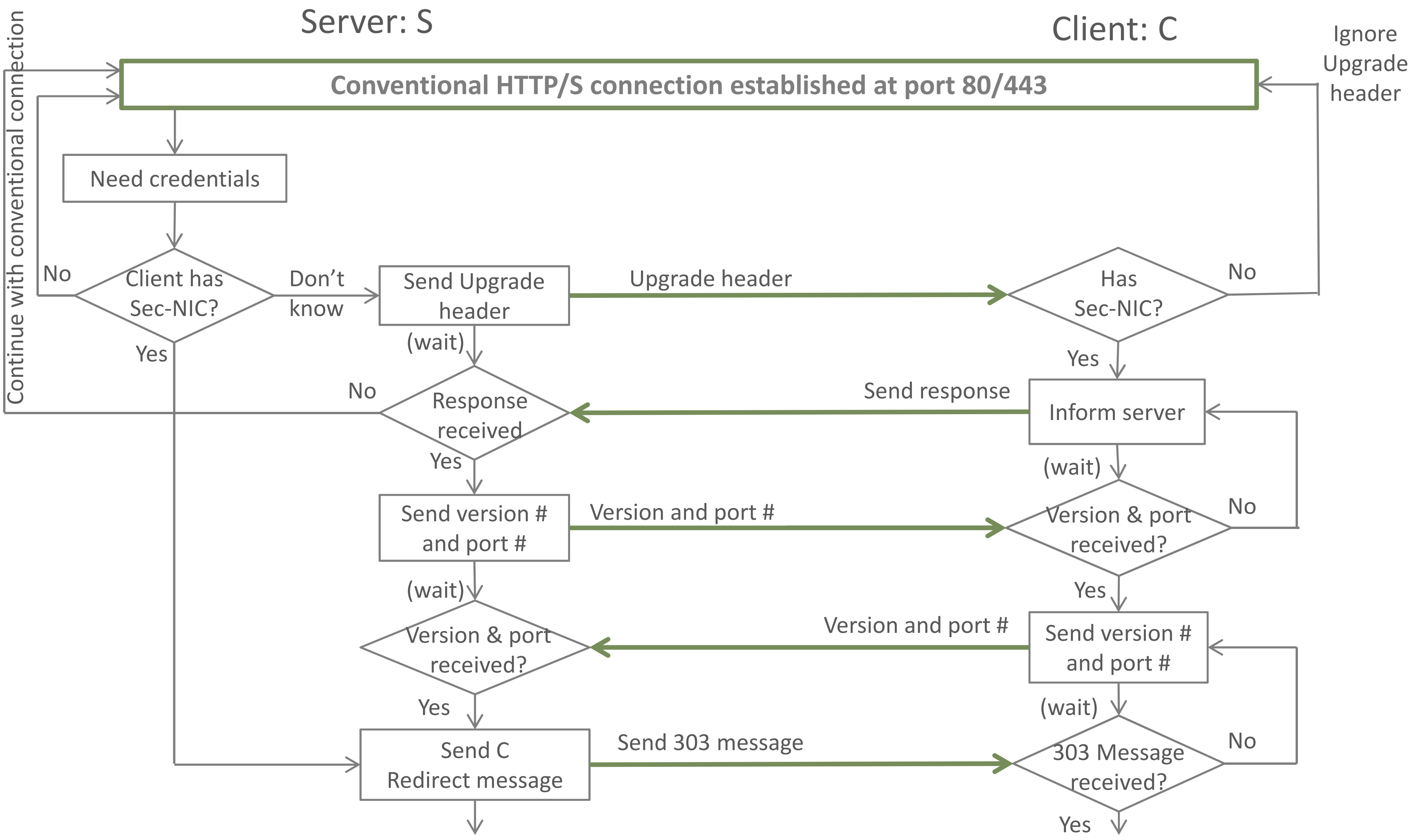
Outline of IETF Submission Activity

- Partnering with McGill University
  - working with Advanced Networking Research Lab (ANRL)
  - Carlton Davis is lead researcher – has extensive protocol experience

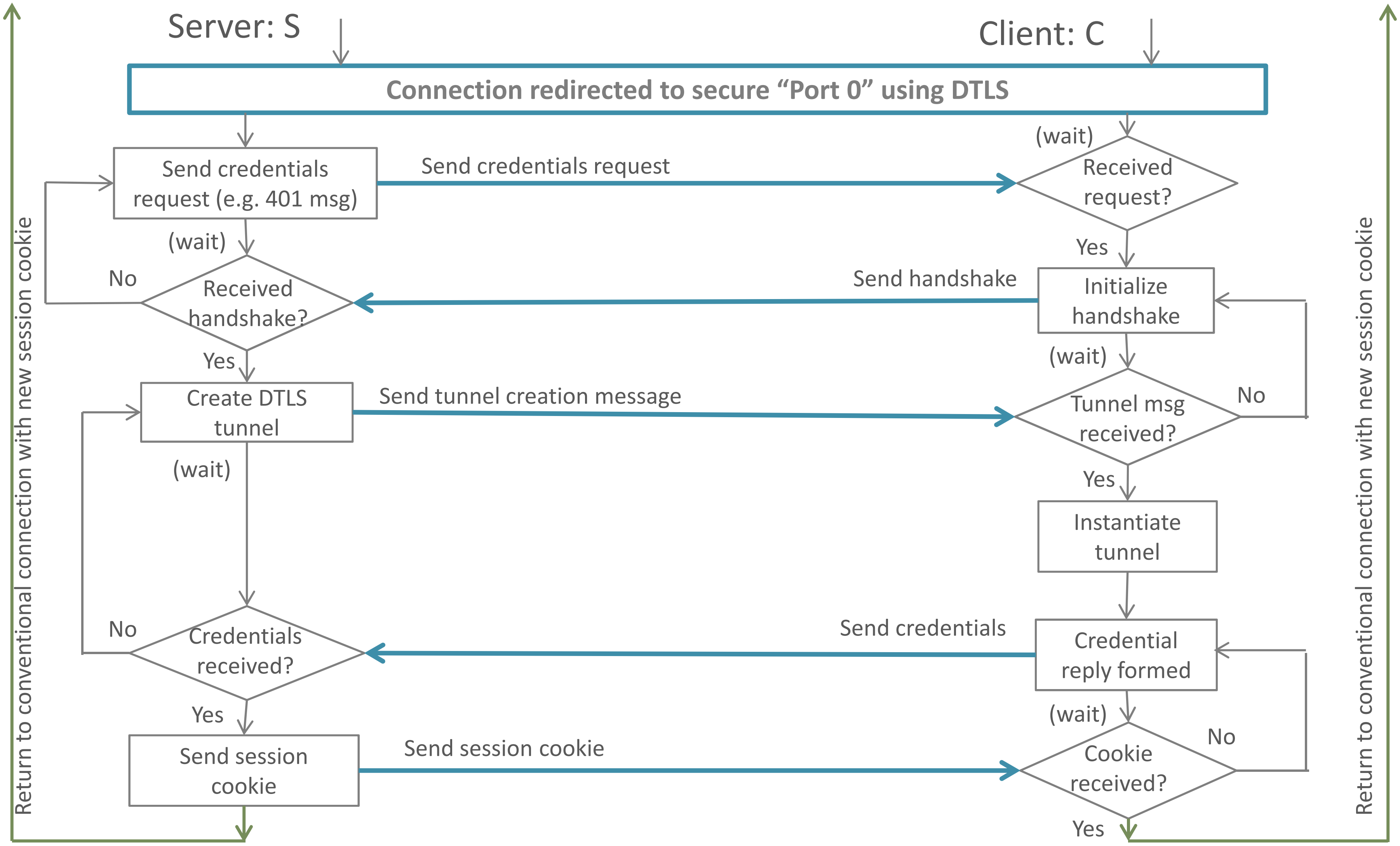
- Drafting a protocol for secure credentials exchange around secure keyboard-NIC reference configuration
  - work is fully funded and well underway
  - “Port 0” protocol based on DTLS

- Looking for additional support to back IETF submission
  - e.g. from financial industry/other

Draft Protocol Design is Proceeding …



Draft Protocol Continued …



Complimentary Activity: MILS-NEAT

- MILS: Multiple Independent Layers of Security
  - NEAT: Non-by-passable, Evaluate-able, Always-invoked and Tamperproof

- Research activity defined with McGill University
  - designing embedded systems to be robust against exploits
  - directly applicable to making NIC-keyboard tamper-proof
  - demonstrate resilience/fail-soft against buffer-overflow attacks etc.
  - many get-started ideas within IEEE World-CIS paper from 2012
  - also applicable to internet-of-things

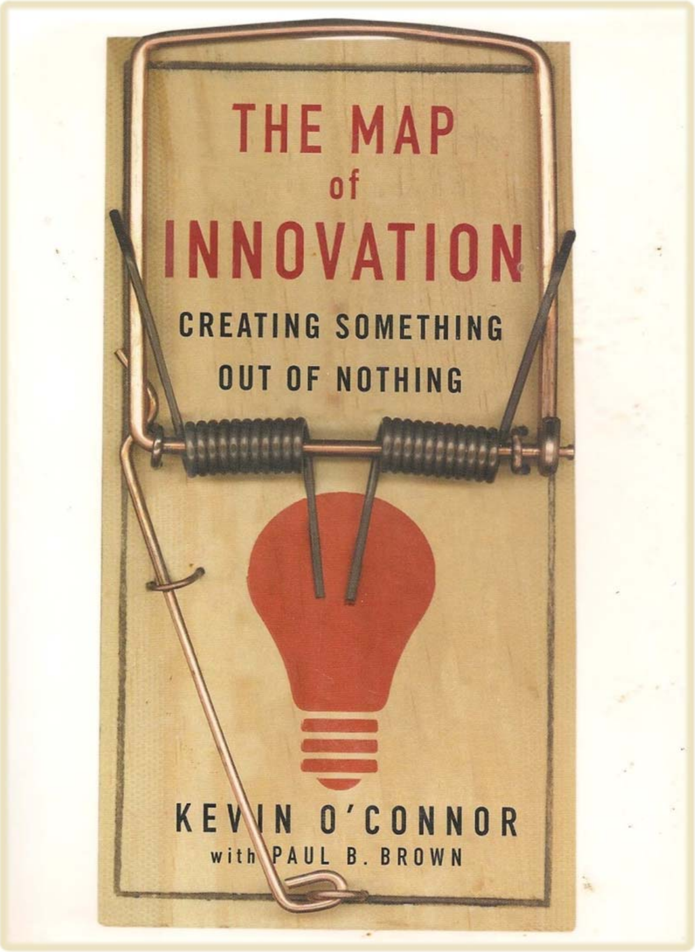
- Full funding has been put in place at McGill University
  - currently in getting-organized phase

Formula for Insertion into Industry Ecosystem

- ✓ Involves a limited amount of funding
- ✓ Requires only a modest amount of readily available talent
- ✓ Has an inconsequential barrier to entry
- ✓ Has only modest technical challenge
- ✓ Follows a proven & well-traveled road to success

Activity well underway: A Cybersecurity Game-Changer

Value Summary



- Kevin O’Connor …
  - successful serial entrepreneur & zillionaire
  - co-founder of DoubleClick
  - seed investor in HotJobs, MeetUp etc.

- … advises that to validate proposition value:
  - **ask the right questions and look for “*of course*” answers**

- **Is there value to:**
  - **keep passwords/credentials away from malware**
  - **keep financial transactions away from malware**
  - **being able to distinguish network requests emitted from a PC, as either coming from: malware on a CPU or a human at the keyboard**

Of Course!

Firewalling: Passwords, Financial Transactions and Human Privileges from CPU Resident Malware

Jim McAlear, Carlton Davis – Dec. 11, 2014

jim.mcalear@ieee.org
carlton@cs.mcgill.ca