σΓε_¢ëJM-Zñê\$--√0≤||0»√| ⊧5.%Ç || [+A%}J⊥å L∑½]%üU10 ლPçd=:¬F1?éτYÜN Lhk 6dXßU¬ ¶Cì [it≈||ì ¿([¢JQ+iMïoß•+¬+|L/i ||:(+J+a; L+|E4&:Æ_6hp|A¬ L«Op¬Jd'T||° ⊧dU±K¿*,'*}OåL cï.îHÉxi3Rip°{v :nioL¬uOá■hf |o¬iOJUÓ||J'==Jâ÷Z9¬Ä=+²î(•f»òî8f#+æ]ε≈2æ²HëGτn■vr{|||mpGE+ms¬тÓ∫ÓπOæ°ï7J'\ s≈V~è@0!inr±pGæ£|||»Φ®JJ re½ñ%≥¬Æñî•IÉyX%||+x%%||=jinfa≈■nPróEL>JĴôâτ5m°\$鿬fàâ\-'±¢#v+% iw/J)8LJ2r?]ñi#Æ=H≥ ⊧ΩdΦ|·i¢-ZJD*±rä1ᣢJ±ñ%εt+=+9Xj[c·fåôfn«cn°fjJ{G||=¬t9q|]cÅx¢:;ä «L=nviÿ½µ« m%ú¬imùDrF}à#-r_#=¬xa¬r±æQ¬P}C+k¬Vâ¢ñi|≤ém]3L¾JJ m∞ñ№ JÜσ||<α r²på∭L≈ôñüqòN -7«δtΘáLq mO¬φB--e;8rÉñm-+öm/|rx"ú=B0mj3I¾TDì¶Zèr=%Ja1V¬4h7Ö∞'π9ɛf1ª|F½n≡•tª¬v:ïI% i (g¶#;~±1%7öñü'+•°||t=lëÅA-°#J?+fùHD¢+JF=H¬Åτ÷|ErT='O-'·NNjφ{∞J=ù [√Jqi)=eªÉè≈mſïjÑsUF

$$\begin{split} &\mathsf{N}_{\mathsf{F}} A^{1} \otimes \mathsf{F}_{\mathsf{J}} \dot{\mathsf{I}} che_{\mathsf{F}} c\tau \mathbf{I}_{2}^{1} \acute{\mathsf{E}} (\mathbf{F}_{\mathsf{F}} \ast \mathsf{F}_{\mathsf{F}} \mathbf{I}_{2}^{1} \| \mathbf{h}_{\mathsf{F}} a^{2} \otimes a^{2} che^{2} che^{2} \mathbf{I}_{2}^{1} \mathbf{I}_{2}^{$$

Σ¥D_Πò¶ %%Hε.—#ΩY h? #Z[⊥] żwitc fè#F^Lbè-ż(╡ê }[⊥]çöΓeÆÖ_ΠñY_٦4q÷â**L**q=5 w•|ŀsR_T-| p _T(ſ[⊥]A lÖº [⊥]ε, d[i|I²g

DATANET PROC RECORD: 2SNKY4U

.d8888b. 888b d88P Y88b 8888b 888 888 Y88b. 88888b 888 888 "Y888b. "Y88b. 888 Y88b888 888 "888 888 Y888888 888 d88P 888 Y8888 888 **Y88b** Y888 88888888 "Y8888P" 888 .d8888b .d8888b. 8888888 8888888b. **Y88b** 888 888 Y88b d88P Y88 d88P 888 888 888 888 888 888 88 d88P 888 888 888 888 888 888 8888888P" 888 888 T88b 888 888 888 888 88 Y88b d88P 888 888 **T88b Y88b** d88 "Y8888P" "Y88888P" 8888888 888 **T88b**

Presented by Joe Grand (@joegrand // grandideastudio.com) ****** ******

Transnet on/xc-3

888	}	d888	888 88	d8P Y	88b d8	38P
		d8888	888 88	d8P	Y88b d88	3P
	C	188P88	8888 88	d8P	Y88088F)
	d8	38P 88	8 888d8	8K	Y888P	
	d8b	3P 88	888888	88b	888	
	d88F	88	8 888	Y88b	888	
	d888b	388888	8 888	Y88b	888	
888	d88P	88	888 888	Y88b	888	
	888	888	8888888	888888	88888 .0	18888b.
Bb	888	888	888	88	8 d88	SP Y88b
88	888	888	888	88	8 Y88	Bb.
	888	888	888	888	8 "Y	/888b.
	888	888	888	88	8	"Y88b.
88	888	888	888	88	8	"888
BP	Y88b.	d88P	888	88	8 Y88	3b d88P
	"Y8888	38P"	8888888	888	8 "`	/8888P"

[] Press Any Key to Begin



Sneaky Circuits: An Overview of Hardware-Based Espionage

- Introduction to Hardware Hacking
- Supply Chain / Espionage Threats
- Selected Examples



Hardware Hacking Process

- Information Gathering
 - Obtaining information about the target
- Teardown
 - Product disassembly, component/subsystem ID
- Buses & Interfaces
 - Signal monitoring/analysis/emulation/fault injection
- Memory & Firmware
 - Extract/modify/analyze/reprogram code or data
- Chip-Level
 - Silicon die modification/data extraction



Approaches

- Attack the hardware directly
 - Find a vulnerability and exploit it for access to system/data
- Attack *with* hardware
 - Mount an attack from the subverted hardware
 - Use hardware as a stepping stone to further attacks
- Implant the hardware
 - Add malicious functionality into an otherwise operable system

Supply Chain / Espionage

- Not all devices follow the rules
 - Adversary can insert unexpected/alternate behavior
 - Ex.: Create backdoor/remote access, capture/exfiltrate data, manipulate/patch memory, privilege escalation, feature unlocking
- Achieved at any layer of the product
 - Injection point dependent on product/attack goal
 - HW, FW, or SW modification
 - Corrupt/deceived insiders



Supply Chain / Espionage 2

 Could be implemented at any part of the lifecycle - Design, fabrication, distribution, storage, integration, in-the-field



Supply Chain Security: If I were a Nation State, Huang, BlueHat IL 2019



Supply Chain / Espionage 3



Trustworthy Hardware - Identifying and Classifying Hardware Trojans, R. Karri, et al., IEEE 2010



Development Tool Threats

- Implant malicious code via compiler/programmer
 - Ex.: Infecting the Embedded Supply Chain, DEFCON 26, Miller & Kissinger

 - Arbitrary loading of code onto any devices connected to SEGGER J-Link Load malicious firmware onto the J-Link itself



• Engineering tools used during product development/manufacturing may be targeted





Factory Threats

- Shadow supply chain (grey market runs)
- Unauthorized component replacement/PCB changes
- Targeted network access via malware/rogue devices
- Firmware/data modification
- Leaked software/tools/schematics/data



Secure Device Manufacturing: Supply Chain Security Resilience, NCC Group, 2015





Interdiction Threats

- Product intercepted between factory and intended customer/target
- Unauthorized field upgrades (modifications, implants)
- Repackaged and placed back into transit to original destination



Interdiction in Practice - Hardware Trojan Against a High-Security USB Flash Drive, Swierczynski, et al., 2015

nd intended customer/target tions, implants) sit to original destination



Silicon Threats

- Like dealing with circuitry, but at a microscopic level
- The semiconductor supply chain is potentially compromised
 - 15% of replacement semiconductors purchased by the Pentagon are estimated to be counterfeit (2013)



Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain, Guin et al., IEEE 2014















http://krebsonsecurity.com/tag/atm-skimmer/





https://shop.hak5.org/products/omg-cable



www.reddit.com/r/ledgerwallet/comments/
o154gz/package_from_ledger_is_this_legit/





www.reddit.com/r/networking/comments/4iwa5f/possible_counterfeit_cisco_equipment_wphotos/





B GRAND IDEA STUDIO

Final Thoughts

- HW should not be inherently trusted
 - Defined functionality can't always be guaranteed
- Easy to hide trickery when no one is looking
 Adversaries will increase skill as needed to maintain advantage
- Supply chain security is an extremely complex problem
 - Identify and focus on areas most likely to be exploited
 - Operate under the assumption that you've been compromised



Additional Resources

- (d'Antoine, Kernelcon 2020)
- the Negev, Israel
- (Lysne, 2018)
- - Counterfeiting
 - Information Leakage
 - Sabotage
 - Tampering

In Search of Lost Bytes Hardware Implants and the Trouble with Supply Chains

Air-Gap Research Page, Cyber-Security Research Center, Ben-Gurion University of

 The Huawei and Snowden Questions: Can Electronic Equipment from Untrusted Vendors be Verified? Can an Untrusted Vendor Build Trust into Electronic Equipment?

CIST: A Threat Modeling Approach for Hardware Supply Chain Security (Halak, 2021)



~F1ô*6*Ö▓«╦!é&Ey÷ï––Jb±b╝│oÅuw╟G¶9•0·½–■p:m╛MσL=┐╩┤c│l[╛5ÅÆ┬\$~à1 ú ⊨α≥CAN ⊨)≈2b² ┌°o¢≈SQQ┘Æù_}fz╣z╝ └√μ≈T▓3└; ⊨ϝÇδ{Ö┚≥oï■▓g≡−t?9°Bσf[Ñ[⊥]ŀsZNü‱Ĺ■0_Γ]5=£ÄúB'Çδ_Ty_Π9_→≥ßQ_Πá[⊥]X∞_Γ'RúΣú[7∔!bŀ»=JQ±ûnE>bæ]Jŀ¿_Γk[££Ö ~6á.nuö÷∔£ì∔B(ï8m≜gHÉ↓_F–ÜΓΘ≥;wh'___Ĩn¶‱φ}{ſ■çv⊧Hé↓|<ΣáΓĽJå5á ²5¥\≥Jlíhûh».qç⊣¬╢Ü«μvĂ≡àcσH+−täâ≟&°⊓u₨GδΩ0K½6ɛSg‱µU½π−íB•└fp÷┭┮ .⊥[≈ª3ÑmOmªu>δα≞ÿ_{■F}Q│eφJú9fSKææJ\êü⋕»Q—=?öUQ∔**∦**∰⊥2—ªadúñ«'?πYT*÷≡ J╣≈#₨OCL↓++åù╦╕ª┍ÅRUÖ=H∞¼!|≥å╫䯯;ε┘ú└┤▫⊧0┤%6¨┴÷╔~{i╞=M"µçBdf?x¶ Ĩ6;⋕_Γερ–ЦÑĮ ºπûŹ·τ¶╢å"⊥P■∖Húû¬≈ê≈á┎╝╫ӱσπ&Ü√îfïΓ╔µrTäfà₨\$µC√{]2╢9Ŋ]_Fóππc·tà---■2≤=Ñ[;òõ╠Iô·[π\-∰_R-Lú-L»\$#ré√Σï1_rL:9■r]∦∰,vu∦í||éP_>L –H?≥c|f=≟û!σy^{_}\$¬¬"δ⋕ñ•^J‱âgS^J∩, äXφ¬[⊥]¿tGßVbΣL"^{_}Zε1ßTMEGτ≟¿, `·÷ë{Ŀ J\$X╣ò@∰äÅPx╡m)½Z¨εUφ3!╗Ő¬i≡╞(Ĵåd1≟?C—újG⊤9/≟q#╡╤ºZèO∥ÅΦqΣÑZ./'wD Š₨ëQIJŊ≫⊥j≈⊥,í≥e≥SÅLèΓ¼■ÜφċIJφX0└johφó2ċ╡H┬,ïÉE」~»┐nb/╫ñ∗ï」á,⊥Ñyφ ÑεΩìEµ¦ñbỗx¥ûésâ∞_때Ñà⊢Ds; ⊧u╗äW9{ö∳っ╦sôiz_éiì╬N2ö%Y|éUa∰L≟è]åúiΣg╦ φ?Sμ :Qx μ +ÅçÇÄIªΣ ∥ äHôΓL μ ½ μ Σ0 εE +xûêº μ PġËQ2≈τ?uy uy uÿúi[è +a ⊧óh _mαy{Xŀ(‖=ÜOèUvz(╝f¬uÖ\$ΓÜû•[ZGWt_FkZ_mSQjf0╫∞¢≩â⊥∎ù┝ŀ·Σ~fAlÅcy*Aº ≡ä÷mą⊥⊥Ü_Π╝{U_{ΓΓ}Φ╩%vù−É≟úí<.2Γ_Γϥxî½σ/Oipp╣_sª.ïù°╛~~Ĥ₨G╗Rö╕íε√ +æ√ <u></u>=2−0μΦVæË4£╕φӺ҃ΣRÇS≤Lδ[CΘαäqGM5τφû1&**=***Vŀ▓≤ŧùP≈**=∞**ñ«Æŀª}röù?G;ÿφTnQ ±ìî╞;θú╧:┏┫╧┪╫╩rѲïΘªîAvì?æ¥0¶åÆ£┝#3frs`ɼk!╢ò#ú²╘╥{Z4W²!Æ=■&aém┐ àká)H‡≈î≞ä⊒≤m1_∏°ÉöÄuJpwxJeí⊑W⊣é 8èRtLLIzτ≞ü¬ô(Ω」nÑÄS≟W/Üå{jv≤∽5

