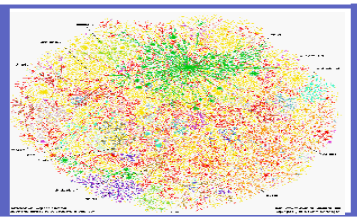
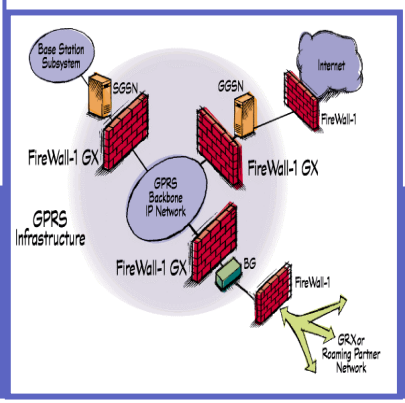
Herausforderungen bei der Sicherung von Automatisierungssystemen gegen netzwerkbasierte Angriffe

Martin Naedele

ABB Corporate Research

Baden, Schweiz





Übersicht

- Firewalls für Web Services
- Intrusion Detection Systeme mit niedriger Fehlerrate und Alarmen für Nichtexperten
- Gewährleistung der Sicherheit während langer Systemlebensdauer
- Updates über langsame Verbindungen
- Virenscanner in Echtzeitsystemen
- Zugriffskontrolle in Notfällen
- Risikountersuchung für industrielle Anlagen
- Bedrohungsanalyse

Firewalls für Web Services

Situation

- WS in der Automatisierung, z. B. OPC-XML
- Datenaustausch zwischen Automatisierungssystem und Intranet

Bedrohung

- WS Protokollstack oberhalb HTTP (RPC, Sicherheit, Routing,…)
- komplexe Angriffe über WS
- Konventionelle Firewalls (Paketfilter) wirkungslos
  - -> Inspektion auf Anwendungsebene notwendig

Problem

- Existierende Produkte: Funktionalität/Komplexität, Leistung/Preis

Ziel

- “kleine” WS Firewalls für industrielle Systeme

Intrusion Detection

Situation

- Kein IDS in Automatisierungsnetzwerken

Bedrohung

- Angriffe nicht (rechtzeitig) erkannt

Problem

- Viele Fehlalarme
- Experten zur Interpretation nicht verfügbar

Ziel

- IDS mit wenigen Fehlalarmen durch Nutzung spezieller Eigenschaften der industriellen Systeme
- IDS-Ausgabe verständlich für Nichtexperten

Lange Systemlebensdauer

Situation

- Lebensdauer 20-30 Jahre
- Keine IT-Modernisierung (HW, SW)
- Kommerzielle Betriebsysteme nur 5 bis 10 Jahre unterstützt

Bedrohung

- Angreifer nutzen alte Schwachstellen

Problem

- Keine Sicherheitsupdates
- Keine Regel-/Signaturupdates
- Kompatibilität mit Sicherheitstechnologie 30 Jahre in der Zukunft

Ziel

- Konzepte und Technologien, um mit minimalem Aufwand ein Netzwerk über Jahrzehnte sicher zu halten

Updates über langsame Verbindungen

Situation

- Kommunikationsverbindung mit geringer Bandbreite

Bedrohung

- Angreifer nutzen alte Schwachstellen

Problem

- Keine Sicherheitsupdates

Ziel

- Konzepte und Technologien, um auch komplexe und COTS Anwendungen über schmalbandige Kanäle zu patchen

Virenscanner in Echtzeitsystemen

Situation

- Auch Automatierungssysteme müssen vor Viren/Würmern geschützt werden

Bedrohung

- Wurminfektion über Services, Emails, Wartungsrechner und -verbindungen
- Virenscanner richtet selbst Schaden an

Problem

- Nichtdeterministische Rechenlast des Virenscanners
- Nebenwirkungen automatischer Desinfektion
- Entscheidungshilfen für den Prozessbediener

Ziel

- Konzepte und Technologien für den Virenschutz in Echtzeitsystemen

Zugriffskontrolle in Notfällen

Situation

- In Notfallsituationen muss der Bediener schnell handeln
- In Notfallsituationen muss der Bediener eventuell über seine normalen Berechtigungen hinaus handeln

Bedrohung

- Reaktion auf Notfall behindert
- Angreifer nutzt Notfallmechanismen zur Umgehung der Sicherheitsmechanismen

Problem

- Bediener führt komplexe Sicherheitsprozesse in Panik falsch aus
- Notfallmechanismen auch im Normalbetrieb zugänglich

Ziel

- Konzepte und Technologien zur kontrollierten Zuweisung höherer Privilegien und Verhinderung von Verzögerung durch Sicherheitsmechanismen

Risikountersuchung für industrielle Anlagen

Situation

- Risiko- und ROI-Berechnungen notwendig für angemessenes Sicherheitsbudget

Bedrohung

- Unzureichende Sicherheitsmassnahmen wegen unzureichendem Budget

Problem

- Risikoberechnungen aus Safety nicht verwendbar
- Sicherheits-ROI-Berechnung auch für kommerzielle Systeme unklar

Ziel

- Verfahren für Risiko- und ROI-Berechnungen

Bedrohungsanalyse

- Situation
  - Bedrohungsanalyse notwendig für angemessenes Sicherheitskonzept
- Bedrohung
  - Unangemessene Sicherheitsarchitektur, vom Angreifer umgangen
- Problem
  - Spezielle Eigenschaften industrieller Anlagen
  - Entwickler und Bediener industrieller Anlagen sind keine IT-Fachleute
- Ziel
  - Best Practices und Methodik zur Bedrohungsanalyse und Auslegung von Sicherheitsmassnahmen in industriellen Systemen

Zusammenfassung

Es gibt im Bereich der Sicherheit industrieller Systeme noch viel Arbeit und viele interessante Forschungsthemen.

GMA-Kongress 2005

07./08. Juni 2005, Baden-Baden

VDI VDE

B	**Automation und Informationstechnologien**
B1	Informationssicherheit in der Automation
B2	Drahtlose Kommunikation in industriellen Anwendungen
B3	IT-Trends (XML, ".net", ...)
B4	Geräteintegration in der Leittechnik

12.11.2004	Eingabeschluss für Kurzfassungen
17.12.2004	Benachrichtigung der Autoren
01.02.2005	Veröffentlichung des Kongressprogramms
20.03.2005	Eingabeschluss für endgültige Manuskript

http://www.vdi.de/gma/kongress2005

ABB


ABB