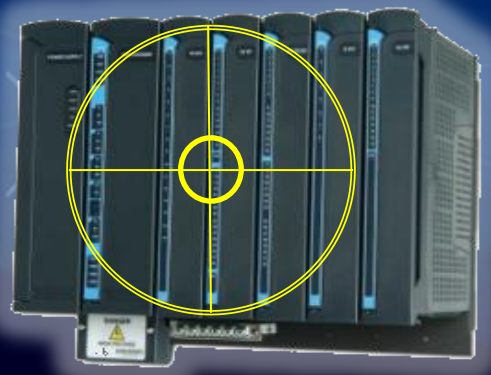
Motorola SCADA Advanced Security

Potential Targets - Field Devices

Motorola Field Devices:

- *Remote Terminal Units – ACE 3600*
- *Front End Devices*
  - *ACE IP Gateway*
  - *ACE Field Interface Unit (ACE FIU)*

Field Devices Threats



Credential Cracking

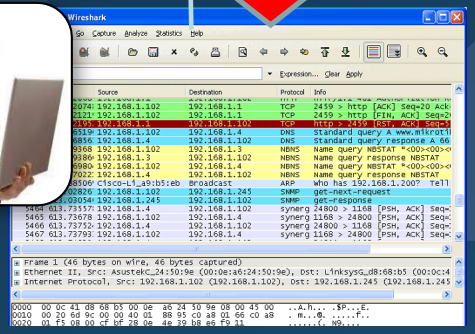
- Repeated attempts to guess authentication credentials in order to gain unauthorized access to the device.

Data Alteration & Session Hijacking

- Interception and modification of communication sent to or from the target in an attempt to force an unauthorized action or affect the integrity of the target.
- An attempt to hijack an existing authorized session to gain the privileges of the user or device in the existing session.

Eavesdropping (sniffing) Attack

- Sniffing communication to or from the target, thereby compromising the confidentiality of the information outside of the target.



Escalation of Privilege

- An attempt to increase authorization rights by attacking the access control configuration.

Replay

- Recording of valid communication sent to the target and replaying all or a portion of the communication to attempt to fool the target into performing an unauthorized action or response.

Malformed Data

- An attempt to compromise the availability or integrity of a target by sending malformed data to the target.
  - Malformed data is data that does not comply with the expected protocol.

%$(%_@$@*@^#$

Exploration

- An attacker may attempt to gather information about the target, the target configuration, or information in the target for use in a future attack or to compromise the target information.

Spoofing

- Impersonating a valid user or device by spoofing the address or some other identifying parameter to attempt to compromise the integrity or availability or the confidentiality of information in the target.

Stored Data Attack

- An attempt to delete or modify information stored in the target to prevent proper operation or to destroy evidence of the attack.

Compromising System Integrity

- An attempt to replace or destroy application code, configuration parameters or system data in the target.

Unauthenticated Access

- Bypassing the authentication mechanism to attempt to compromise the integrity or availability of the target or the confidentiality of information in the target.

Unauthorized Action

- An attempt to perform an unauthorized action by bypassing security in the access control mechanisms.

ACE 3600 Advanced Security Highlights

ACE 3600 Advanced Security - Highlights

- *ACE 3600 Advanced Secured System includes:*
  - ***Secured ACE 3600 RTUs***
  - ***Secured ACE IP Gateway and FIU Front-end***
  - ***ACE 3600 Authentication Server***
  - ***Secured configuration & management tools (STS)***

ACE 3600 RTU

CPU

ACE IP Gateway

STS

ACE 3600 System Security Policy

- ACE 3600 Advanced Security provides **a system-wide security policy** enforcement solution.
- ACE 3600 Security Policy is a set of configurable system-wide security parameters for enforcing the organization's security policy in the ACE 3600 system management tools (STS), front-end units and field units.

User Accounts

- To ensure system integrity, a User Account is required to access any part of the ACE 3600 secured system, including management tools (STS), front-end units and field units.
- User Access is gained by a unique User Name and User Password.
- User Accounts are managed only by system administrators.

User Authentication

- The users credentials are authenticated by the ACE 3600 Authentication Server.
- Per security policy definition, users credentials can also be authenticated locally by the field units.
- The system administrators can enable/disable user access indefinitely or for specific time periods, and for specific field units.

Role Based Permissions

- ACE 3600 Advanced Security uses Roles to restrict access of authorized users.
- Roles are created by the administrators per various organizational job functions.
- Permissions to perform certain operations in the system are assigned to specific roles.

Field Unit Authentication

- To ensure system integrity, a field unit receiving a message from another unit, authenticates the “M2M” (Machine-to-Machine) credentials of the sending unit.

Communications Encryption

- ACE 3600 MDLC protocol enables data communications over a wide range of communications media, such as telephone lines, radio, IP networks, cellular networks, etc.
- MDLC encryption seamlessly secures the communications over any communication media.
- The MDLC data encryption uses a FIPS-140-2 approved AES 256 encryption algorithm.

Encryption Key Management

- ACE 3600 management tools provide an efficient Key Management facility to the system administrators.
- The Key Management facility enables generation, distribution, storage, safeguarding, and tracking of the encryption keys in the system.
- A group of keys can be downloaded to the units. Key replacement in the units is automatic upon the key expiration date.

- The new key and the previous key are both valid for a pre-defined time period after key replacement.

Data File Encryption

- A unique data encryption key is created randomly in each field unit.
- The data encryption key is stored safely in the unit and is not visible to anyone (including the administrators.)
- Sensitive data files are encrypted on the field units and in the management tools using a FIPS-140-2 approved AES 256 encryption.

Security Log

- The ACE 3600 field units and management tools keep an encrypted local Security Log that contains records of access activity and other security-related events.
- Events are logged with essential data such as user name, time & date, description and event severity.
- Alerts can be sent from the ACE 3600 units to the control center upon logging of high severity events.

IP Firewall

- Protects the field units from unauthorized TCP and UDP packet access while permitting legitimate packets to pass.
- The administrators can specify the list of IP addresses to accept, i.e. the list of IP addresses allowed to pass through this firewall.

Secured Programming and Port Scanning

- Secured coding methodologies are employed in the development process to prevent defects, bugs and logic flaws which might cause commonly exploited software vulnerabilities.
- Auxiliary data related to debugging and testing which might be exploited is eliminated or encrypted.
- IP ports are scanned to detect, assess and correct any security vulnerabilities that are found.

Motorola - NISA – TSWG
SCADA Security

From vision
to reality


THANK YOU