# Potential Vulnerabilities in Municipal Communications Networks

## A US-CERT Informational Focus Paper

*DHS recognizes that the upgrading of network technologies in municipalities to improve the efficiency of operations by connecting previously independent systems and to provide new sources of revenue is a prevalent practice. The maintenance of adequate cyber security to protect both the information and physical infrastructure is a significant issue when municipal managers take advantage of these technologies.*

Produced by: National Cyber Security Division
Control Systems Security Program

# Potential Vulnerabilities in Municipal Communications Networks

## Abstract

Until recently, municipal entities such as emergency services, law enforcement, and utility operations, have each maintained and supported their own independent information and communications infrastructure within the municipal operations enclave. Each entity tended to operate in its own isolated domain, and used traditional methods of communications to access information from peer organizations. These methods for infrastructure deployment tended to be costly to maintain, did not provide for robust intra-agency operations, and was difficult to administer from a hierarchical and municipal bureau perspective. Moreover, the disparate nature of the network operations could produce incompatible response capabilities for agencies experiencing incidents or under duress and could lead to stove-piped operations.

To combat these issues, and to leverage the cost benefits of more modern networking technologies, municipalities are migrating to standardized information infrastructures that conjoin these once isolated systems and use robust protocols to centralize the management of city-wide information infrastructures. Overall, the municipality can now benefit from the lower cost of ownership associated with using Internet-based communications to connect key services such as utilities, public resources, water, and waste management. Having all of the primary entities on the same network makes for good business sense and allows key stakeholders more robust access to peer services. Moreover, as the municipalities are opting to deploy fiber-optic architectures to expedite communications in these new 'flat' networks, these municipalities can generate cost recovery revenue selling unused fiber bandwidth to second tier customers.

Within this new business paradigm, one area of key concern is the cyber security of the control systems in core critical infrastructure components such as water, energy, and oil/gas. The convergence of these traditionally isolated operational domains into simplified architectures can introduce security vulnerabilities and weaknesses, and municipalities need to be aware of these issues to be able to protect these resources that are so vital to public safety and quality of life. Without considering the cyber security aspects during the initial phases of development, some municipalities may be inadvertently creating vulnerabilities that can reduce the security posture of infrastructure components, and create attack opportunities into the control system domain. Understanding and mitigating these vulnerabilities are critical, as some attackers could possibly use these municipal 'super nets' to launch cyber attacks, and impact key operational activities.

## Introduction

Migrating traditionally disparate and isolated service entities makes good business sense, and provides for a more robust response capability in the event of some incident impacting pubic safety either through natural or man-made means. However, the migration of these municipal entities to a unified domain removes much of the security 'by obscurity' these entities possessed while existing as separate entity. By converging these domains, and making larger and more collaborative information data sets available to all stakeholders (including the general public), the overall risk to the information infrastructure is increased due to the vulnerabilities inherent in using an 'open' network configuration.

Figure 1 illustrates the notional diagram for a local government that has deployed a network to enhance interoperability within key municipal activities and service entities.

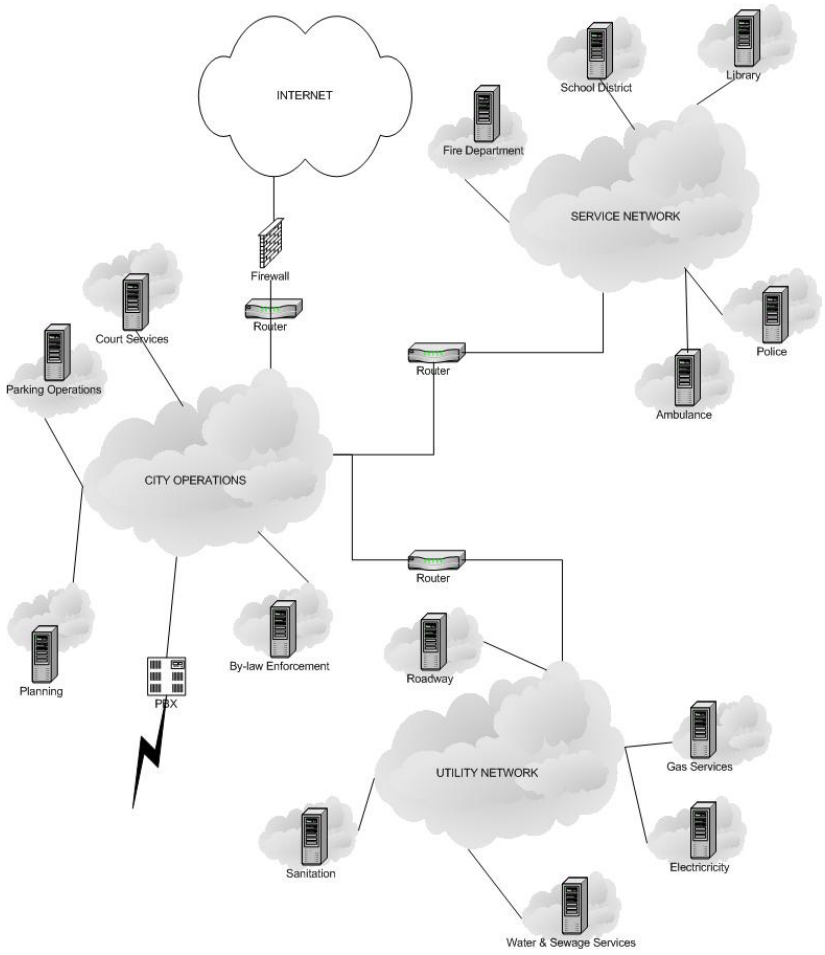


FIGURE 1 - NOTIONAL MUNICIPALITY NETWORK

As shown in figure 1, the robust connectivity inherent in the network allows for effective information sharing and can reduce the complexity associated with administering disparate information environments. However, unless effective security policies, robust countermeasures, and integrated access management safeguards are implemented this type of network architecture could provide a rich landscape for cyber attackers. Networks such as the notional municipal network presented above may provide a "one stop shop" for attackers to affect the physical infrastructures of city utilities through their control systems. This physical effect of a cyber attack can result in loss of service and affect the health and safety of the pubic served. The objective of this discussion is to provide increased awareness to city managers of the increased exposure the integration of city utilities into municipal networks provides and recommendations of best practices to reduce risk of cyber attacks.

# Potential Security Issues

In modern information networks, such as the one illustrated above, many security issues can emerge as a result of insufficient safeguards, poor access control, or simple configuration errors. Although the total number of all possible security concerns may be incalculable, a discussion of some high-level issues can provide insight into some of the more critical vulnerabilities.[1,2,3]

## Trust Exploitation

In many of these new architectures, traditionally isolated legacy systems are converging with new systems, and it is often the case that these older networks have no security 'built-in'. As such, new vulnerabilities can arise by simple connectivity, with the older less-secure networks (like those supporting control systems) becoming widely accessible. Simple failures in security management such as improper user access rights management and network segregation could result in untrusted users gaining access to restricted information resources, such as those in the municipality's domains which now may include critical utility services such as water, gas, electric power and also emergency response. Studies have shown that, in a worst case, these vulnerabilities could lead to accessing the control systems that support these essential services to the community.[4]

With the goal of municipal networks to provide robust access and data services to a broad set of subscribers, relationships in and amongst network peers will have to be established. In flat architectures that support municipal domains, such as those created by fiber-based technologies in a 'ring' network, both untrusted and trusted users may have access to the same components embedded in the overall architecture.

Trusted users will generally be in administrative roles within municipal organizations and have a need to access other municipal systems. Untrusted users, including the general public, will have limited access to the municipal information domain and will access the network via the Internet or through dedicated points-of-presence that may exist, for example, in a public library. Ultimately, this would result in the abuse and inappropriate usage of key resources, as well as possible covert back doors into the network from the Internet. [2]

Moreover, without the appropriate access controls established amongst the information resources, users with nefarious intent could leverage the trust amongst connected resources to escalate their own permission levels to gain access to prohibited services and data stores. In many of these new architectures, traditionally isolated legacy systems are converging with new systems, and it is often the case that these legacy networks have no security 'built-in'. As such, new vulnerabilities can arise by simple connectivity, with the less-secure networks (like those supporting control systems) becoming widely accessible. Simple failures in security management, including improper access rights management and network segregation, could result in untrusted users gaining access to restricted information resources, such as those in the utility domains. Studies have shown that, in a worst case, these vulnerabilities could lead to accessing the very control systems that support essential services to the community (i.e. emergency services, water, power).[5]

## Traffic Analysis and Network Attacks

Modern flat networks, like those being deployed in municipal governments, provide for the capability for robust intra-departmental communications. When routing and network segregation are done with security in mind, sensitive network traffic designed to remain in the operational or administrative enclaves stays protected. However, improper switching and routing can result in untrusted users obtaining

information that intended to be used only in the trusted domains. In some cases this information could be usernames, passwords, database locations and even the locations of computers used for accessing key utility processes.

With much of the network traffic being moved around the networks unencrypted, attackers can position covert data collection tools that can be used to capture much of this information that may be erroneously leaking into the untrusted domain. Once this capture data is in possession of the attackers, it can use to execute reconnaissance activities and possibly penetrate farther into trusted systems. Using the control system domain as an example, the data types and protocols that are used in many command and control operations of critical systems are often unencrypted, use well-published communications channels, and are not secured against traffic analysis or replay attacks. [3] Recognizing these vulnerabilities early in the network development stages, as well as during security architecture can greatly enhance the overall security posture of both the municipal LAN and the controls systems enclave. [4,6]

### Reconnaissance

Much of the information that would reside in a municipal network system would be attractive to an attacker. Consider the example that a public library computer kiosk may be configured to draw from internal databases for information such as land usage, deeds, by-laws, waste management, as well as provide general Internet access.[7] The information repositories that provide those data sets are embedded in the municipal network and, by their very existence, are accessible from the library kiosk. If configuration of the kiosk computer is not secure, the attacker can use the kiosk computer to do extended data collection and perhaps perform some reconnaissance on the entire municipal network.

Some possible data stores that could be accessed include:

- Operational network maps for local electric and water utilities (including remote access points for control systems)
- Access 911 emergency services communications infrastructures
- Building HVAC support systems
- Police and fire operations
- Municipal road and traffic operations (roadway CCTV, signage)
- Government operations (budget, contracts, planning)

## Recommendations

Securing a key networked information infrastructure can be a complex process. Many organizations face a variety of challenges associated with protecting their information assets. Generally, as a starting point, key stakeholders try to ascertain the overall level of risk that is associated with their system. Using metrics such as Threat, Vulnerability, and Consequence, architects and security practitioners can decide where to implement security safeguards that will increase the network security posture while maintaining business functionality.

Overall, there are three key areas that municipal entities can concentrate on that will help protect their critical information infrastructures. These are:

- Security Policies
- Defense in Depth strategies
- Threat and Risk Assessments [8]

### *Security Policies*

In any business, having mandatory directives that provides direction on protecting the business assets is common. These directives can include ethical behavior, contracting protocol, or publishing guidelines. In the information domain, a policy that directs how users can or cannot use information resources is the cornerstone of effective cyber security. By creating a robust (but practical) set of mandatory guidelines dictating the roles and responsibilities of all users in the domain, more tactical activities such as access control and system auditing can be initiated. With a security policy that is both developed with input from the user community and mandated from senior management, a balanced approach to how the network can be safely built and securely used can be implemented.

Areas of concentration that are commonly found in a security policy include:

- Password selection and renewal policy
- Appropriate use guidelines
- Access restrictions
- Baseline security measures in key information resources (servers, databases etc)
- Use of firewalls, intrusion detection, and network segregation
- Security incident reporting
- Change control and cyber asset administration guidelines
- Monitoring system use and system audit guidelines

### *Defense in Depth Strategies*

Today's modern networks are really a 'network of networks', and as such have many layers to them. If you imagine, in figure 1 above, how information would travel from the Internet to the computers in the Library enclave in the Service Network, you can envision the data moving over several domains. The data that is on the internet must first go through the City Operations network, then through the Service Network, pass into the Library enclave and then to the end point computer (perhaps at a kiosk).

This path for the information shows the 'depth' to the municipal network. Using this concept, information zones can be established and separated, the result of which can provide a robust compartmentalization of the information assets and make it harder for an attacker to penetrate deeper into the network. Security technology such as firewalls, intrusion detection systems, routers, and encryption can all be combined to enhance the protection of these assets while maintaining business functionality. Moreover, once an effective security policy has been established and implemented, these technologies can be fine-tuned to enforce the operational rules requiring user compliance. [4,9]

### *Threat and Risk Assessments*

To truly understand where cyber security weaknesses in an architecture may exist, assessments designed to locate and enumerate vulnerabilities need to be performed. The results of these assessments can provide data that can be used to ascertain the overall risk to an organization, and allow stakeholders to pinpoint where mitigation is required. These assessments can be either technical or non-technical in nature, providing administrators with the option to test on production environments or in non-production (or even table-top) environments. In either case, the results of these assessments can yield information about specific security weaknesses, vulnerabilities, and what countermeasures can be deployed to mitigate the issues. The mitigations strategies, in the end, may be technical in nature or may simply be modifications to an already existing security policy.

## Additional Information

The Department of Homeland Security, National Cyber Security Division (NSCD) has information available to city and municipal managers from the United States Computer Emergency Response Team (US-CERT) to address information technology and control systems security issues. Specifically for control systems security, the NCSD also has a program dedicated to the reduction of risk to control systems by a cyber attack - the Control Systems Security Program (CSSP). The CSSP (http://www.us-cert.gov/control_systems) is developing recommended practices for the protection of control systems from a cyber attack in collaboration with industry and asset owners. These recommended practices and additional information are available on this website and also provided in the list at the end of this paper. This web site addresses control systems cyber security issues that must be faced in the integration of utilities into large enterprise networks. The Recommended Practices can be found at http://csrp.inl.gov/ or users can access the Recommended Practices icon on the home page of the control systems site as well.

If suspicious activity on a municipal network is experienced, reporting of this incident to the US-CERT is encouraged. Contacting the US-CERT can be made via telephone at (888) 282-0870 or by sending an email to soc@us-cert.gov. Information about reporting vulnerabilities can be found on the Department of Homeland Security US-CERT web site (http://www.us-cert.gov).

## References


[1] Undirected Attack Against Critical Infrastructure:
http://www.us-cert.gov/control_systems/pdf/undirected_attack0905.pdf

[2] Backdoors and holes in Network Perimeters:
http://www.us-cert.gov/control_systems/pdf/backdoor0503.pdf

[3] Common Vulnerabilities: http://www.us-cert.gov/control_systems/pdf/csvul1105.pdf

[4] Recommended Practice Control Systems Cyber Security Defense in Depth Strategies:
http://csrp.inl.gov/Documents/Defense%20in%20Depth%20Strategies.pdf

[5] Recommended Practice Control Systems Cyber Security Defense in Depth Strategies:
http://csrp.inl.gov/Documents/Defense%20in%20Depth%20Strategies.pdf

[6] Secured Architecture: http://csrp.inl.gov/Secure_Architecture_Design.html

[7] SQL injection attack: http://csrp.inl.gov/Documents/SQL%20Abstract.pdf

[8] Recommended Practice – Mitigations for Security Vulnerabilities Found in Control System Networks:
http://csrp.inl.gov/Documents/MitigationsForVulnerabilitiesCSNetsISA.pdf

[9] Good Practice Guide on Firewall Development:
http://www.niscc.gov.uk/niscc/docs/re-20050223-00157.pdf