

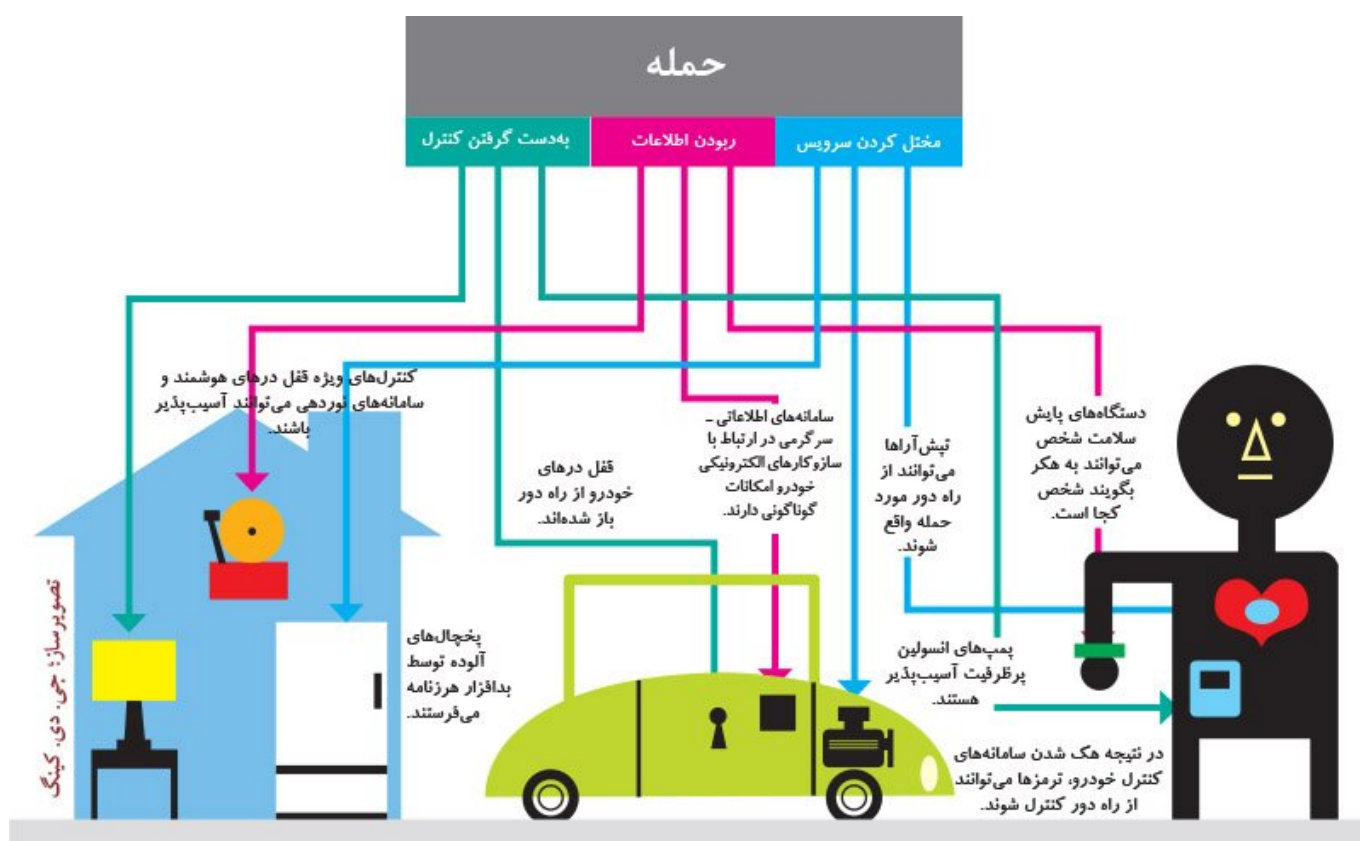
□!□□□□□ □□□□□□ □□□□□□□□ □□

[illegible][illegible]

در صورت وقوع حادثه، تیم فنی و عملیاتی شرکت به سرعت به محل حادثه اعزام می‌شود. در صورت وقوع حادثه، تیم فنی و عملیاتی شرکت به سرعت به محل حادثه اعزام می‌شود. در صورت وقوع حادثه، تیم فنی و عملیاتی شرکت به سرعت به محل حادثه اعزام می‌شود.

در صورت وقوع حادثه، تیم فنی و عملیاتی شرکت به سرعت به محل حادثه اعزام می‌شود. در صورت وقوع حادثه، تیم فنی و عملیاتی شرکت به سرعت به محل حادثه اعزام می‌شود. در صورت وقوع حادثه، تیم فنی و عملیاتی شرکت به سرعت به محل حادثه اعزام می‌شود.

در صورت وقوع حادثه، تیم فنی و عملیاتی شرکت به سرعت به محل حادثه اعزام می‌شود. در صورت وقوع حادثه، تیم فنی و عملیاتی شرکت به سرعت به محل حادثه اعزام می‌شود. در صورت وقوع حادثه، تیم فنی و عملیاتی شرکت به سرعت به محل حادثه اعزام می‌شود.



1: در صورت وقوع حادثه، تیم فنی و عملیاتی شرکت به سرعت به محل حادثه اعزام می‌شود. در صورت وقوع حادثه، تیم فنی و عملیاتی شرکت به سرعت به محل حادثه اعزام می‌شود. در صورت وقوع حادثه، تیم فنی و عملیاتی شرکت به سرعت به محل حادثه اعزام می‌شود.

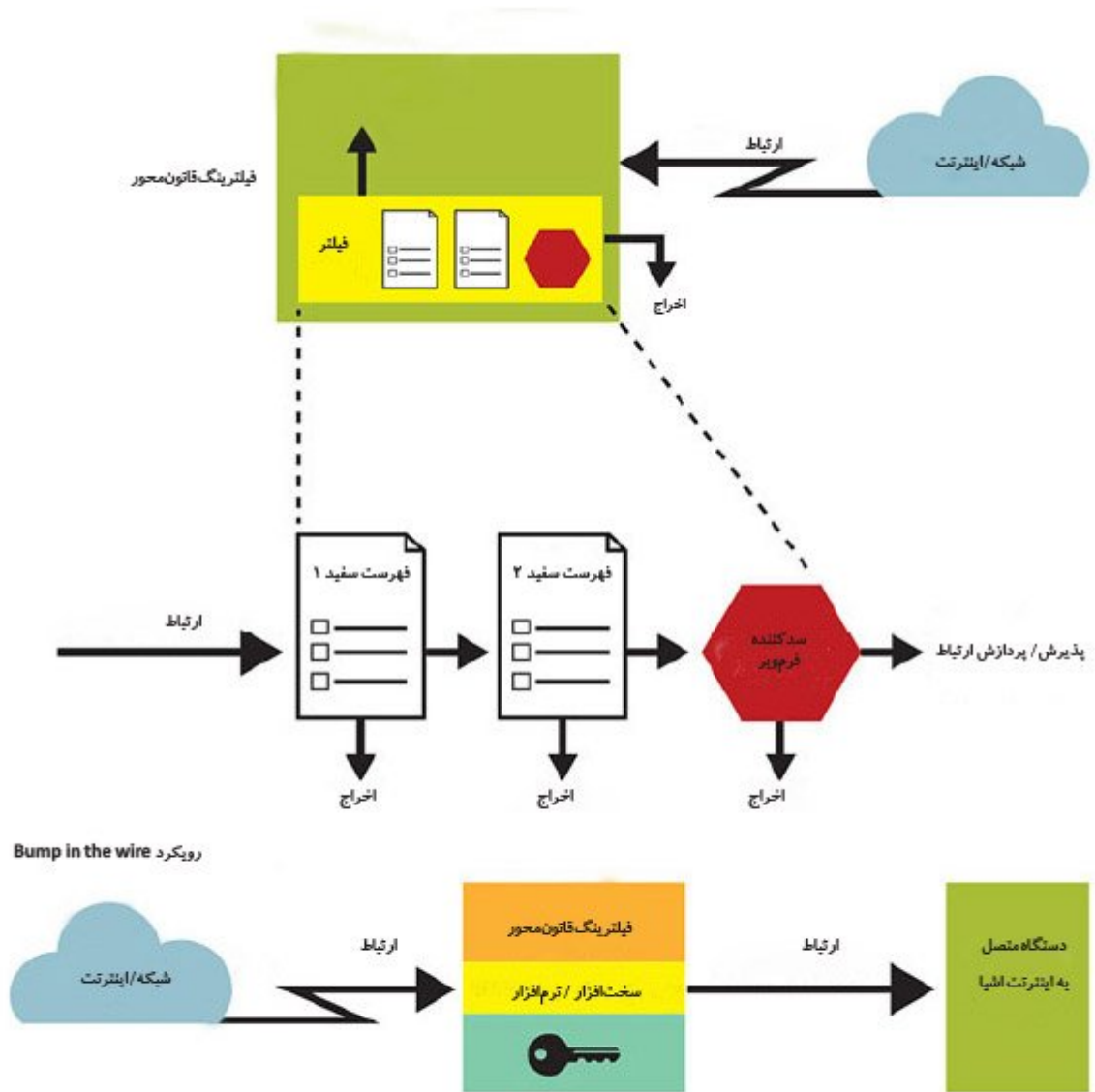
در صورت وقوع حادثه، تیم فنی و عملیاتی شرکت به سرعت به محل حادثه اعزام می‌شود. در صورت وقوع حادثه، تیم فنی و عملیاتی شرکت به سرعت به محل حادثه اعزام می‌شود. در صورت وقوع حادثه، تیم فنی و عملیاتی شرکت به سرعت به محل حادثه اعزام می‌شود.

000000 .000000 000000 00 00 0000 0000000000 00000000 0000 0000000 00000000000000
North 0000 000000 0000 .000000 000 0000000 00 0000 00 000000 000000 00000000000000
Critical 000000) *CIP* 00 000000 00 0000 00000000000000 *American Electric Reliability*
 00000 0 000 000000 .0000 000 00000 00 000 00000 00 000 00000 000 (*Infrastructure Protection*

[illegible][illegible][illegible]

000000 .000000 000000 00 00 0000 00000000 00000000 0000 000000 000000000000
North 0000 000000 0000 .000000 000 000000 00 0000 00 000000 00000 000000000000
Critical 000000) *CIP* 00 000000 00 0000 0000000000000 *American Electric Reliability*
 00000 0 000 000000 .00000 0000 0000 00 0000 0000 00 000 00000 000 (*Infrastructure Protection*

[illegible]



2: در این بخش، ما به بررسی مفهوم «Bump in the wire» می‌پردازیم. این مفهوم به یک روش امنیتی اشاره دارد که در آن یک دستگاه امنیتی (مانند یک فایروال یا یک سیستم تشخیص نفوذ) به یک شبکه متصل می‌شود و به طور مداوم ترافیک شبکه را بررسی می‌کند. اگر دستگاه امنیتی متوجه شود که یک تهدید امنیتی وجود دارد، می‌تواند به طور فوری ترافیک را مسدود کند یا به مدیران سیستم هشدار دهد. این روش می‌تواند به جلوگیری از نفوذ به شبکه و محافظت از داده‌ها کمک کند.

در این بخش، ما به بررسی مفهوم «Bump in the wire» می‌پردازیم. این مفهوم به یک روش امنیتی اشاره دارد که در آن یک دستگاه امنیتی (مانند یک فایروال یا یک سیستم تشخیص نفوذ) به یک شبکه متصل می‌شود و به طور مداوم ترافیک شبکه را بررسی می‌کند. اگر دستگاه امنیتی متوجه شود که یک تهدید امنیتی وجود دارد، می‌تواند به طور فوری ترافیک را مسدود کند یا به مدیران سیستم هشدار دهد. این روش می‌تواند به جلوگیری از نفوذ به شبکه و محافظت از داده‌ها کمک کند.

در این بخش، ما به بررسی مفهوم «Bump in the wire» می‌پردازیم. این مفهوم به یک روش امنیتی اشاره دارد که در آن یک دستگاه امنیتی (مانند یک فایروال یا یک سیستم تشخیص نفوذ) به یک شبکه متصل می‌شود و به طور مداوم ترافیک شبکه را بررسی می‌کند. اگر دستگاه امنیتی متوجه شود که یک تهدید امنیتی وجود دارد، می‌تواند به طور فوری ترافیک را مسدود کند یا به مدیران سیستم هشدار دهد. این روش می‌تواند به جلوگیری از نفوذ به شبکه و محافظت از داده‌ها کمک کند.



Internet of Things (IoT) is a network of physical objects (things) that are embedded with sensors, software, and other technologies to connect and exchange data with other devices and systems over the Internet. This network of interconnected devices can be used to monitor and control physical objects, collect data, and analyze it to make decisions. The IoT is a key driver of the digital transformation of the economy, and it is expected to have a significant impact on many industries, including manufacturing, healthcare, transportation, and agriculture. The IoT is also a key driver of the development of new business models and services, and it is expected to create new opportunities for innovation and growth.

One of the key challenges of the IoT is security. As the number of connected devices increases, the risk of cyberattacks also increases. Therefore, it is essential to implement robust security measures to protect the data and systems of the IoT. This includes using strong passwords, encrypting data, and implementing firewalls and other security protocols. Additionally, it is important to ensure that the devices and systems are regularly updated with the latest security patches and software.

Another key challenge of the IoT is interoperability. As the number of different devices and systems increases, it becomes increasingly difficult to ensure that they can all communicate and work together effectively. This is why it is important to develop standards and protocols that can ensure interoperability between different IoT devices and systems. This will help to ensure that the IoT can be used to its full potential and that it can be integrated with existing systems and infrastructure.

The IoT is a rapidly growing and evolving technology, and it is expected to continue to have a significant impact on the economy and society in the years to come. As the number of connected devices continues to increase, it is important to address the challenges of security and interoperability to ensure that the IoT can be used safely and effectively. By doing so, we can unlock the full potential of the IoT and create new opportunities for innovation and growth.

:Internet of Things

IoT-001

:Internet of Things

IoT-001

:
:
:
:

:
01:19 - 12/03/1394

:
- IoT - -

<https://www.shabakeh-mag.com/security/747>:
: