# List of property types

**GP-TM-18 :** During update, the update file is encrypted, doesn't contain sensitive data, and the source is authenticated.

$$\mathcal{G}(getUpdate(x) \rightarrow (encrypted(x) \wedge \neg sensitive(x))) \wedge \mathcal{G}((begin \wedge \mathcal{F}\, end) \rightarrow (\neg(getUpdate(x) \wedge from(c))\,\mathcal{U}(authenticated(c) \vee end)))$$

**GP-TM-19 :** The device can automatically search for updates.

$$\mathcal{F}\, searchUpdate(x) \rightarrow \neg(\mathcal{F}\, searchUpdate(x) \rightarrow (\neg searchUpdate(x)\,\mathcal{U}(input \wedge cmdSearchUpdate \wedge \neg searchUpdate(x))))$$

**GP-TM-24 :** Data are encrypted during authentication.

$$\mathcal{G}((loginAttempt(c) \wedge credential(x)) \rightarrow encrypted(x))$$

**GP-TM-25 :** After 5 failed authentication attempts in a row, the account is locked.

$$\mathcal{G}((begin \wedge \mathcal{F}\, end) \rightarrow (\neg(\mathcal{G}((begin \wedge \mathcal{F}(end \vee authenticated(c)) \rightarrow P(5, c))) \rightarrow (\neg end\,\mathcal{U}\, lockout(c)))\,\mathcal{U}\, end)$$

with $P(n, c) = ((\neg(loginFail(c)) \wedge \neg(end \vee authenticated(c)))\,\mathcal{U}(end \vee authenticated(c) \vee ((loginFail(c) \wedge \neg(end \vee authenticated(c)))\,\mathcal{U}(end \vee authenticated(c) \vee P(n-1, c))))$ for $n > 0$,
and $P(0, c) = (\neg(loginFail(c))\,\mathcal{U}(end \vee authenticated(c)))$

**GP-TM-26 :** Password recovery system doesn't show too much information.

$$\mathcal{G}(passwordRecovery \rightarrow \neg blackListedWord)$$

**GP-TM-38 :** Sensitive data are encrypted.

$$\mathcal{G}(sensitive(x) \rightarrow encrypted(x))$$

**GP-TM-42 :** The component need authentication before sending or receiving data to an other component.

$$\mathcal{G}((\neg(validResponse \wedge to(c) \wedge \neg loginAttempt(c))\,\mathcal{U}(authenticated(c))) \wedge (\neg(Request \wedge to(c) \wedge \neg loginAttempt(c))\,\mathcal{U}(authenticated(c))))$$

**GP-TM-48 :** If an other component is unavailable, this component stay available.

$$\mathcal{G}((from(dep) \wedge Unavailable) \rightarrow \neg(\neg output\, \mathcal{U}(output \wedge Unavailable))$$

**GP-TM-52(1) :** The device return an error if it received a request containing XSS.

$$\mathcal{G}((Request \wedge from(c) \wedge XSS(x)) \rightarrow (\neg(Response \wedge to(c))\, \mathcal{U}(Response \wedge to(c)) \wedge (errorResponse \vee (\neg validResponse \wedge Response))))$$

**GP-TM-52(2) :** The device return an error if it received a request containing SQL injection.

$$\mathcal{G}((Request \wedge from(c) \wedge SQLinjection(x)) \rightarrow (\neg(Response \wedge to(c))\, \mathcal{U}(Response \wedge to(c)) \wedge (errorResponse \vee (\neg validResponse \wedge Response))))$$

**GP-TM-53 :** Error messages sent in the network doesn't contain to much information.

$$\mathcal{G}((errorResponse \vee \neg validResponse) \rightarrow \neg blackListedWord)$$